P-663H-51

ADSL2+ Pair Bonding 4-port Router

User's Guide

Version 1.00
10/2007
Edition 1

DEFAULT LOGIN	
IP Address	**http://192.168.1.1**
User Name	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

It is recommended you use the web configurator to configure the ZyXEL Device.

- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

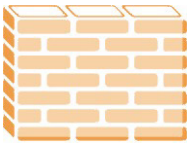
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-663H-51 may be referred to as the "ZyXEL Device", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

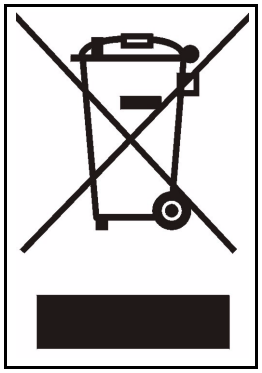
ZyXEL Device	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Switch	Router

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Please use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction 23

Introducing the ZyXEL Device 25
Introducing the Web Configurator 31
Initial Configuration 37
Device Information 39

Advanced 49

WAN Setup 51
LAN Setup 67
Network Address Translation (NAT) Screens 73
Security 81
Quality of Service (QoS) 89
Routing 97
RIP 101
DNS Setup 103
Dynamic DNS Setup 105
DSL Setup 109
Port Mapping 111

Diagnostics and Management 115

Diagnostics 117
Settings 119
Logs 123
SNMP 127
Time 131
Access Control 133
Update Software 137
Save/Reboot and Logout 139

Troubleshooting and Specifications 141

Troubleshooting 143
Product Specifications 147

Appendices and Index 153

Table of Contents

About This User's Guide **3**

Document Conventions **4**

Safety Warnings **6**

Contents Overview **9**

Table of Contents **11**

List of Figures **17**

List of Tables **21**

Part I: Introduction **23**

Chapter 1
Introducing the ZyXEL Device **25**

1.1 Overview 25
1.2 Ways to Manage the ZyXEL Device 26
1.3 Good Habits for Managing the ZyXEL Device 26
1.4 Hardware Connections 27
1.4.1 Connecting POTS Splitters 27
1.4.2 Telephone Microfilters 28
1.5 System Startup and LEDs 28

Chapter 2
Introducing the Web Configurator **31**

2.1 Web Configurator Overview 31
2.2 Accessing the Web Configurator 31
2.2.1 User Access 32
2.2.2 Administrator Access 32
2.3 Resetting the ZyXEL Device 33
2.3.1 Using the Reset Button 33
2.4 Navigating the Web Configurator 33

Chapter 3
Initial Configuration **37**

3.1 WAN Configuration 37

3.2 QoS Configuration 38
3.3 Changing the Login Password 38

Chapter 4
Device Information 39

4.1 Device Information Summary 39
4.2 WAN Information 40
4.3 LAN Statistics 41
4.4 WAN Statistics 41
4.5 ATM Statistics 42
4.6 ADSL Statistics 44
4.7 ADSL BER Test 46
4.8 Route Info 47
4.8.1 DHCP Table 47

Part II: Advanced 49

Chapter 5
WAN Setup 51

5.1 WAN Overview 51
5.1.1 VPI and VCI 51
5.1.2 Multiplexing 51
5.2 Traffic Shaping 51
5.2.1 ATM Traffic Classes 52
5.3 WAN 53
5.4 WAN ATM PVC Configuration and QoS 54
5.5 Connection Types 55
5.5.1 PPPoA 56
5.5.2 PPPoE 56
5.5.3 MER 56
5.5.4 IPoA 56
5.5.5 Bridging 56
5.6 Encapsulation 56
5.6.1 LLC-based Encapsulation 57
5.6.2 VC-based Encapsulation 57
5.7 WAN Connection Type and Encapsulation Mode 57
5.8 NAT 58
5.9 Nailed-Up Connection (PPP) 58
5.10 PPPoA WAN Connection Setup 58
5.11 PPPoE WAN Connection Setup 60
5.12 MER WAN Connection Setup 61

5.13 IPoA WAN Connection Setup 63
5.14 IGMP Multicast 63
5.15 NAT, IGMP Multicast, and WAN Service 64
5.16 WAN Setup Summary 65

Chapter 6
LAN Setup 67

6.1 LAN Overview 67
6.1.1 LAN, WAN and the ZyXEL Device 67
6.1.2 DHCP Setup 68
6.2 LAN TCP/IP 68
6.2.1 IP Address and Subnet Mask 68
6.3 Multicast 69
6.4 Introducing Universal Plug and Play 69
6.4.1 How do I know if I'm using UPnP? 70
6.4.2 NAT Traversal 70
6.4.3 Cautions with UPnP 70
6.5 LAN Setup 70

Chapter 7
Network Address Translation (NAT) Screens 73

7.1 NAT Overview 73
7.2 NAT Virtual Servers 73
7.2.1 Virtual Server: Services and Port Numbers 73
7.2.2 Virtual Servers Example 74
7.3 Configuring Virtual Servers 74
7.3.1 Virtual Server Rule Add 75
7.4 Port Triggering 77
7.5 Port Triggering Add 78
7.6 DMZ Host 80

Chapter 8
Security 81

8.1 Outgoing IP Filtering 81
8.2 Adding Outgoing IP Filtering Rules 82
8.3 Incoming IP Filtering 82
8.4 Adding Incoming IP Filtering Rules 83
8.5 MAC Filtering 84
8.6 MAC Filtering Rules 86
8.7 Parental Control (Blocking Schedule) 86
8.8 Adding Parental Control (Blocking Schedule) Entries 87

Chapter 9
Quality of Service (QoS) 89

9.1 QoS Overview 89
9.1.1 IEEE 802.1Q Tag 89
9.1.2 IP Precedence 90
9.1.3 DiffServ 90
9.2 Configuring QoS General Screen 91
9.3 Queue Configuration 92
9.4 Adding a Queue 92
9.5 Class Setup 93
9.5.1 Configuring a QoS Class 95

Chapter 10
Routing 97

10.1 Default Gateway Setup 97
10.2 Static Route 98
10.3 Configuring Static Route 98
10.3.1 Static Route Add 99

Chapter 11
RIP 101

11.1 RIP Setup 101

Chapter 12
DNS Setup 103

12.1 DNS Server Address 103
12.2 DNS Setup 103

Chapter 13
Dynamic DNS Setup 105

13.1 Dynamic DNS Overview 105
13.1.1 DYNDNS Wildcard 105
13.2 Dynamic DNS 105
13.3 Configuring Dynamic DNS 106

Chapter 14
DSL Setup 109

14.1 DSL Setup 109

Chapter 15
Port Mapping 111

15.1 Port Mapping Setup 111
15.2 Adding a Port Mapping 112

Part III: Diagnostics and Management 115

Chapter 16
Diagnostics 117

16.1 Diagnostics 117

Chapter 17
Settings 119

17.1 Backup Configuration Using the Web Configurator 119
17.2 Restore Configuration Using the Web Configurator 119
17.3 Restoring Factory Defaults 120

Chapter 18
Logs 123

18.1 Logs Overview 123
18.2 System Log 123
18.3 Viewing the System Log 123
18.4 Configuring Log Settings 124

Chapter 19
SNMP 127

19.1 SNMP 127
19.1.1 Supported MIBs 128
19.2 SNMP Screen 129

Chapter 20
Time 131

20.1 Time Setup 131

Chapter 21
Access Control 133

21.1 Access Control Screen 133
21.2 Service Access Control Screen 133
21.3 IP Addresses 134
21.4 Adding IP Addresses 135
21.5 Passwords 135

Chapter 22
Update Software 137

22.1 Uploading Firmware 137

Chapter 23
Save/Reboot and Logout 139

23.1 Save/Reboot 139
23.2 Logout 139

Part IV: Troubleshooting and Specifications 141

**Chapter 24
Troubleshooting 143**

24.1 Power, Hardware Connections, and LEDs 143
24.2 ZyXEL Device Access and Login 144
24.3 Internet Access 145

**Chapter 25
Product Specifications 147**

25.1 DSL Connector Pin Assignments 150
25.2 Power Adaptor Specifications 150

Part V: Appendices and Index 153

Appendix A Setting up Your Computer's IP Address 155
Appendix B IP Addresses and Subnetting 171
Appendix C Pop-up Windows 181
Appendix D Common Services 185
Appendix E Legal Information 189
Appendix F Customer Support 193
Index 199

List of Figures

Figure 1 Protected Internet Access Applications 25
Figure 2 LAN-to-LAN Application Example 26
Figure 3 Hardware Connections 27
Figure 4 Connecting a Microfilter 28
Figure 5 Front Panel 29
Figure 6 Password Screen 32
Figure 7 User Status Screen 32
Figure 8 Web Configurator: First Screen 33
Figure 9 Advanced Setup > WAN > Add 37
Figure 10 Management > Access Control > Passwords 38
Figure 11 Device Info > Summary 39
Figure 12 Device Info > WAN 40
Figure 13 Device Info > Statistics > LAN 41
Figure 14 Device Info > Statistics > WAN 41
Figure 15 Device Info > Statistics > ATM 42
Figure 16 Device Info > Statistics > ADSL 44
Figure 17 Device Info > Statistics > ADSL > ADSL BER Test 46
Figure 18 Device Info > Statistics > ADSL > ADSL BER Test: Results 46
Figure 19 Device Info > Route 47
Figure 20 Device Info > DHCP 48
Figure 21 Example of Traffic Shaping 52
Figure 22 Advanced Setup > WAN 53
Figure 23 Advanced Setup > WAN > Add 54
Figure 24 Advanced Setup > WAN > Add (2) 57
Figure 25 Advanced Setup > WAN > Add (3: PPPoA) 58
Figure 26 Advanced Setup > WAN > Add (3: PPPoE) 60
Figure 27 Advanced Setup > WAN > Add (3: MER) 62
Figure 28 Advanced Setup > WAN > Add (3: IPoA) 63
Figure 29 Advanced Setup > WAN > Add (4: MER) 64
Figure 30 Advanced Setup > WAN > Add (Summary: MER) 66
Figure 31 LAN and WAN IP Addresses 67
Figure 32 Advanced Setup > LAN 71
Figure 33 Multiple Servers Behind NAT Example 74
Figure 34 Advanced Setup > NAT > Virtual Servers 74
Figure 35 Advanced Setup > NAT > Virtual Servers > Add 76
Figure 36 Trigger Port Forwarding Process: Example 77
Figure 37 Advanced Setup > NAT > Port Triggering 78
Figure 38 Advanced Setup > NAT > Port Triggering > Add 79

Figure 39 Advanced Setup > NAT > DMZ Host 80
Figure 40 Advanced Setup > Security > IP Filtering > Outgoing 81
Figure 41 Advanced Setup > Security > IP Filtering > Outgoing > Add 82
Figure 42 Advanced Setup > Security > IP Filtering > Incoming 83
Figure 43 Advanced Setup > Security > IP Filtering > Incoming > Add 84
Figure 44 Advanced Setup > Security > MAC Filtering 85
Figure 45 Advanced Setup > Security > MAC Filtering > Add 86
Figure 46 Advanced Setup > Security > Parental Control 87
Figure 47 Advanced Setup > Security > Parental Control > Add 88
Figure 48 Advanced > Quality of Service 91
Figure 49 Advanced > Quality of Service > Queue Configuration 92
Figure 50 Advanced > Quality of Service > Queue Configuration > Add 93
Figure 51 Advanced > Quality of Service > QoS Classification 94
Figure 52 QoS Class Configuration 95
Figure 53 Advanced Setup > Routing > Default Gateway 97
Figure 54 Example of Static Routing Topology 98
Figure 55 Advanced > Routing > Static Route 98
Figure 56 Advanced > Routing > Static Route > Add 99
Figure 57 Advanced Setup > Routing > RIP 101
Figure 58 Advanced Setup > DNS > DNS Server 104
Figure 59 Advanced Setup > DNS > Dynamic DNS 105
Figure 60 Advanced Setup > DNS > Dynamic DNS > Add 106
Figure 61 Advanced > DSL 109
Figure 62 Advanced Setup > Port Mapping 111
Figure 63 Advanced Setup > Port Mapping > Add 112
Figure 64 Diagnostics 117
Figure 65 Management > Settings > Backup 119
Figure 66 Management > Settings > Update 119
Figure 67 Temporarily Disconnected 120
Figure 68 Management > Settings > Restore Default 120
Figure 69 Management > System Log 123
Figure 70 Management > System Log > View System Log 124
Figure 71 Management > System Log > Configure System Log 124
Figure 72 SNMP Management Model 127
Figure 73 SNMP 129
Figure 74 Management > Internet Time 131
Figure 75 Management > Access Control > Services 133
Figure 76 Management > Access Control > IP Addresses 134
Figure 77 Management > Access Control > IP Addresses > Add 135
Figure 78 Management > Access Control > Passwords 136
Figure 79 Management > Update Software 137
Figure 80 Network Temporarily Disconnected 138
Figure 81 Management > Save/Reboot 139

Figure 82 DSL Connector Pin Assignments 150
Figure 83 WIndows 95/98/Me: Network: Configuration 156
Figure 84 Windows 95/98/Me: TCP/IP Properties: IP Address 157
Figure 85 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 158
Figure 86 Windows XP: Start Menu 159
Figure 87 Windows XP: Control Panel 159
Figure 88 Windows XP: Control Panel: Network Connections: Properties 160
Figure 89 Windows XP: Local Area Connection Properties 160
Figure 90 Windows XP: Internet Protocol (TCP/IP) Properties 161
Figure 91 Windows XP: Advanced TCP/IP Properties 162
Figure 92 Windows XP: Internet Protocol (TCP/IP) Properties 163
Figure 93 Macintosh OS 8/9: Apple Menu 164
Figure 94 Macintosh OS 8/9: TCP/IP 164
Figure 95 Macintosh OS X: Apple Menu 165
Figure 96 Macintosh OS X: Network 166
Figure 97 Red Hat 9.0: KDE: Network Configuration: Devices 167
Figure 98 Red Hat 9.0: KDE: Ethernet Device: General 167
Figure 99 Red Hat 9.0: KDE: Network Configuration: DNS 168
Figure 100 Red Hat 9.0: KDE: Network Configuration: Activate 168
Figure 101 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 169
Figure 102 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 169
Figure 103 Red Hat 9.0: DNS Settings in resolv.conf 169
Figure 104 Red Hat 9.0: Restart Ethernet Card 169
Figure 105 Red Hat 9.0: Checking TCP/IP Properties 170
Figure 106 Network Number and Host ID 172
Figure 107 Subnetting Example: Before Subnetting 174
Figure 108 Subnetting Example: After Subnetting 175
Figure 109 Conflicting Computer IP Addresses Example 179
Figure 110 Conflicting Computer IP Addresses Example 179
Figure 111 Conflicting Computer and Router IP Addresses Example 180
Figure 112 Pop-up Blocker 181
Figure 113 Internet Options: Privacy 182
Figure 114 Internet Options: Privacy 183
Figure 115 Pop-up Blocker Settings 183

List of Tables

Table 1 Front Panel LEDs 29
Table 2 Web Configurator Screens Summary 34
Table 3 Device Info > Summary 39
Table 4 Device Info > WAN 40
Table 5 Device Info > Statistics > LAN 41
Table 6 Device Info > Statistics > WAN 42
Table 7 Device Info > Statistics > ATM 42
Table 8 Device Info > Statistics > ADSL 45
Table 9 Device Info > Route 47
Table 10 Device Info > DHCP 48
Table 11 Advanced Setup > WAN 53
Table 12 Advanced Setup > WAN > Add 55
Table 13 Advanced Setup > WAN 57
Table 14 Advanced Setup > WAN > Add (3: PPPoA) 59
Table 15 Advanced Setup > WAN > Add (3: PPPoE) 60
Table 16 Advanced Setup > WAN > Add (3: MER) 62
Table 17 Advanced Setup > WAN > Add (3: IPoA) 63
Table 18 Advanced Setup > WAN > Add (4: MER) 65
Table 19 Advanced Setup > LAN 71
Table 20 NAT Port Forwarding 75
Table 21 Advanced Setup > NAT > Virtual Servers > Add 76
Table 22 Advanced Setup > NAT > Port Triggering 78
Table 23 Advanced Setup > NAT > Port Triggering > Add 79
Table 24 Advanced Setup > NAT > Port Triggering > Add 80
Table 25 Advanced Setup > Security > IP Filtering > Outgoing 81
Table 26 Advanced Setup > Security > IP Filtering > Outgoing > Add 82
Table 27 Advanced Setup > Security > IP Filtering > Incoming 83
Table 28 Advanced Setup > Security > IP Filtering > Incoming > Add 84
Table 29 Advanced Setup > Security > MAC Filtering 85
Table 30 Advanced Setup > Security > MAC Filtering > Add 86
Table 31 Advanced Setup > Security > Parental Control 87
Table 32 Advanced Setup > Security > Parental Control > Add 88
Table 33 IEEE 802.1p Priority Level and Traffic Type 90
Table 34 Advanced > Quality of Service 91
Table 35 Advanced > Quality of Service > Queue Configuration 92
Table 36 Advanced > Quality of Service > Queue Configuration > Add 93
Table 37 Advanced > Quality of Service > QoS Classification 94
Table 38 QoS Class Configuration 95

Table 39 Advanced Setup > Routing > Default Gateway 97
Table 40 Advanced > Routing > Static Route 99
Table 41 Advanced > Routing > Static Route > Add 99
Table 42 Advanced Setup > Routing > RIP 102
Table 43 Advanced Setup > DNS > DNS Server 104
Table 44 Advanced Setup > DNS > Dynamic DNS 106
Table 45 Advanced Setup > DNS > Dynamic DNS > Add 106
Table 46 Advanced > DSL 109
Table 47 Advanced Setup > Port Mapping 111
Table 48 Advanced Setup > Port Mapping > Add 113
Table 49 Management > Settings > Update 120
Table 50 Management > System Log > View System Log 124
Table 51 Management > System Log > Configure System Log 125
Table 52 SNMP Commands 128
Table 53 SNMP 129
Table 54 Management > Internet Time 131
Table 55 Management > Access Control > Services 133
Table 56 Management > Access Control > IP Addresses 134
Table 57 Management > Access Control > IP Addresses > Add 135
Table 58 Management > Access Control > Passwords 136
Table 59 Management > Update Software 137
Table 60 Device Specifications 147
Table 61 Firmware Specifications 147
Table 62 Standards Supported 149
Table 63 North American Plug Standards 150
Table 64 European Plug Standards 150
Table 65 United Kingdom Plug Standards 150
Table 66 IP Address Network Number and Host ID Example 172
Table 67 Subnet Masks 173
Table 68 Maximum Host Numbers 173
Table 69 Alternative Subnet Mask Notation 173
Table 70 Subnet 1 175
Table 71 Subnet 2 176
Table 72 Subnet 3 176
Table 73 Subnet 4 176
Table 74 Eight Subnets 176
Table 75 24-bit Network Number Subnet Planning 177
Table 76 16-bit Network Number Subnet Planning 177
Table 77 Commonly Used Services 185

PART I
Introduction

Introducing the ZyXEL Device (25)
Introducing the Web Configurator (31)

1

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

The ZyXEL Device is an ADSL2+ pair bonding gateway that allows super-fast Internet access over analog (POTS) telephone lines. It bonds two ADSL2+ lines into a single logical connection to provide increased throughput at longer distances.

In the ZyXEL Device product name, “H” denotes an integrated 4-port switch (hub).

See Chapter 25 on page 147 for a full list of features.

Model names ending in “1”, for example P-663H-51, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service).

The DSL RJ-11 (ADSL over POTS models) connects to your ADSL-enabled telephone lines.

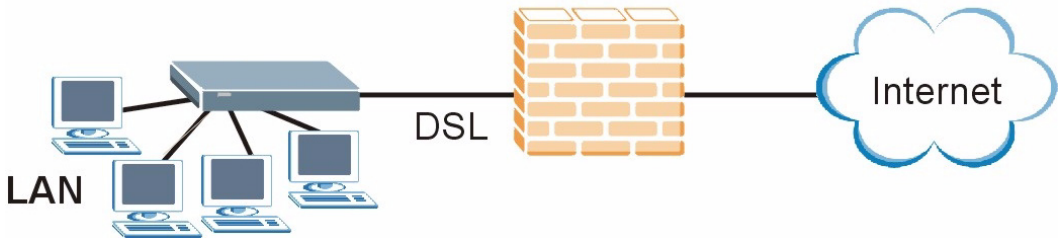
Only use firmware for your ZyXEL Device’s specific model. Refer to the label on the bottom of your ZyXEL Device.

The ZyXEL Device is the ideal high-speed Internet access solution. It supports the ADSL standards listed in Table 61 on page 147.

The ZyXEL Device provides protection from attacks by Internet hackers. By default, the firewall blocks all incoming traffic from the WAN.

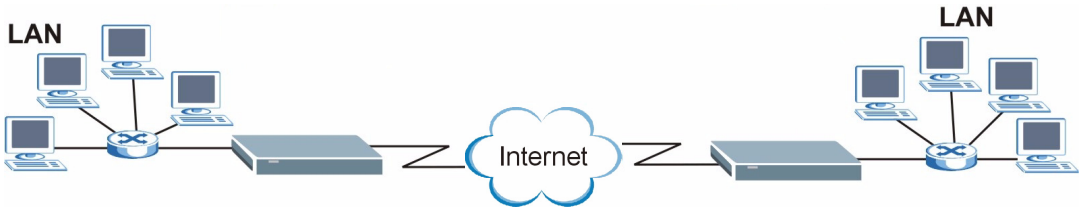
A typical Internet access application is shown below

Figure 1 Protected Internet Access Applications



You can also use the ZyXEL Device to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application example is shown as follows.

Figure 2 LAN-to-LAN Application Example



The ZyXEL Device is compatible with the ADSL/ADSL2/ADSL2+ standards. Using ADSL2+, the ZyXEL Device can attain a maximum downstream rate of about 44 Mbps.[1]

The standard your ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, line quality, etc.

1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. Use this for everyday management of the ZyXEL Device using a (supported) web browser.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

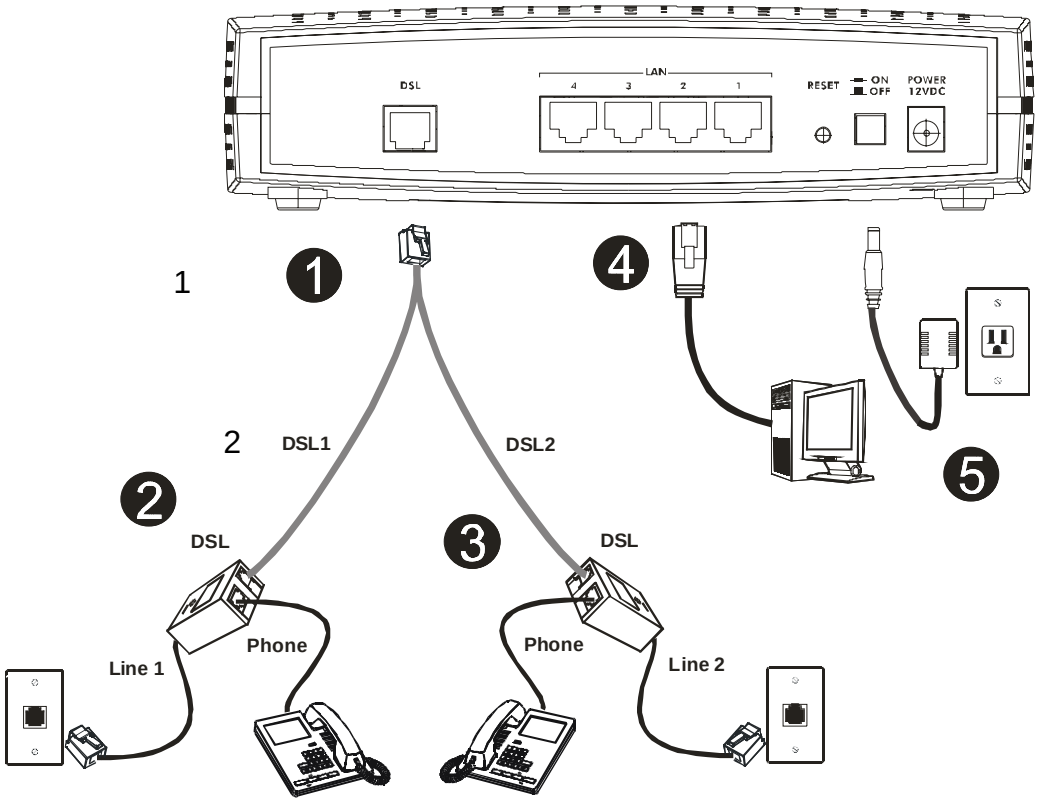
- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

1. This is the theoretical maximum rate under ideal conditions.

1.4 Hardware Connections

Connect the ZyXEL Device as shown next.

Figure 3 Hardware Connections



1. Connect the included DSL Y-cable. Connect the part where the two cables come together connects to the ZyXEL Device's **DSL** port.
2. Connect the **DSL1** end of the Y-cable to the wall jack for your first DSL line. Connect the **DSL2** end of the Y-cable to the wall jack for your second DSL line. If you are using DSL splitters, see Section 1.4.1 on page 27 for details.
3. Use an Ethernet cable to connect a computer to one of your ZyXEL Device's **LAN** ports.
4. Slide the included power adaptor's plug into the power adaptor so that it snaps into place. Then use the included power adaptor to connect the ZyXEL Device's **POWER 12VDC** socket to an appropriate power outlet.

1.4.1 Connecting POTS Splitters

Use POTS (Plain Old Telephone Service) splitters to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitters at the point where the telephone lines enter your premises.

1. Connect the side labeled "Phone" to your telephone.

2 Connect the side labeled “Modem” or “DSL” to your ZyXEL Device.

3 Connect the side labeled “Line” to the telephone wall jack.

1.4.2 Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.

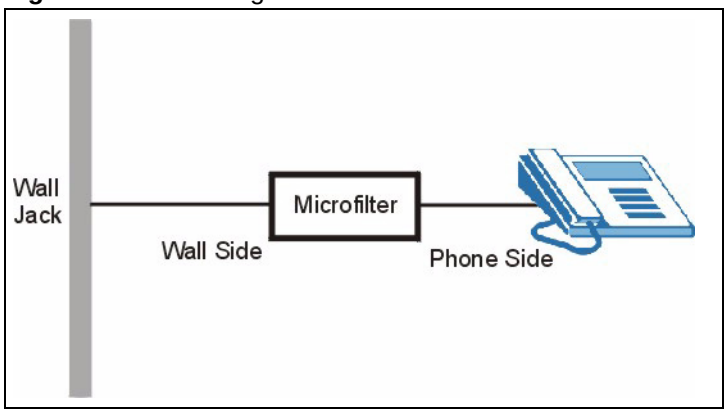
1 Locate and disconnect each telephone.

2 Connect a cable from the wall jack to the “wall side” of the microfilter.

3 Connect the “phone side” of the microfilter to your telephone as shown in the following figure.

4 After you are done, make sure that your telephone works. If your telephone does not work, disconnect the microfilter and contact either your local telephone company or the provider of the microfilter.

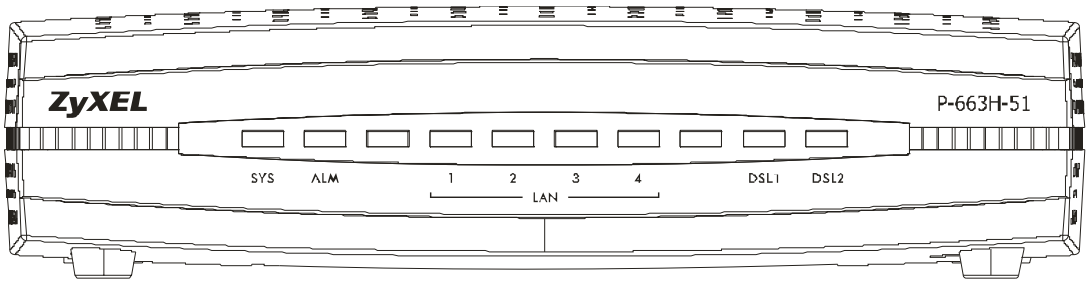
Figure 4 Connecting a Microfilter



1.5 System Startup and LEDs

After you are done making the hardware connections, press the power button to the **ON** position. Look at the LEDs (lights) on the front panel. The following figure shows the ZyXEL Device’s LEDs.

Figure 5 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
SYS	Green	On	The ZyXEL Device is receiving power.
ALM	Red	On	The ZyXEL Device has malfunctioned
LAN 1,2,3,4	Green	On	The ZyXEL Device has a successful Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
		Off	The ZyXEL Device is not connected to the LAN.
DSL1, DSL2	Green	On	The respective DSL line is up.
		Blinking	Fast blinking means the ZyXEL Device is initializing the respective DSL line. Slow blinking means the respective DSL line is down.

2

Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyXEL Device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

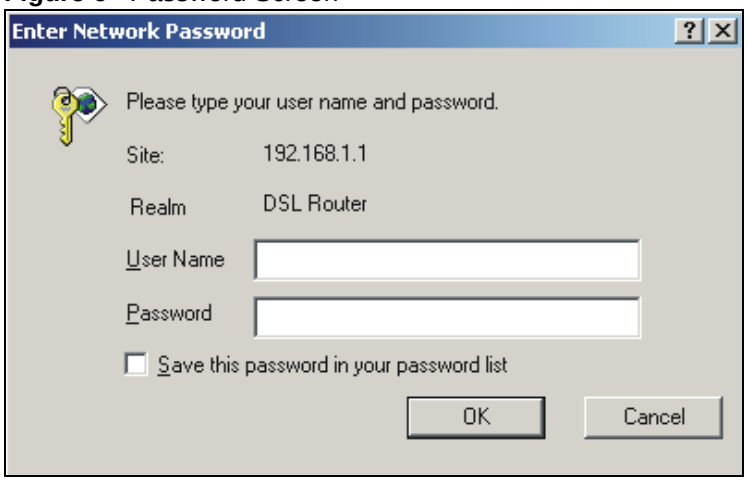
In order to use the web configurator you need to allow web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2. See Appendix C on page 181 if you need to make sure pop-ups are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

The following describes how to access the ZyXEL Device from the LAN using the administrator or user account. See Section 21.5 on page 135 for information about the support account.

1. Make sure your ZyXEL Device hardware is properly connected (see Section 1.4 on page 27).
2. Assign your computer a static IP address (choose one from 192.168.1.2 to 192.168.1.254). See Appendix A on page 155 for how to change your computer's IP address.
3. Launch your web browser.
4. Type "192.168.1.1" as the URL.
5. A screen displays as shown.

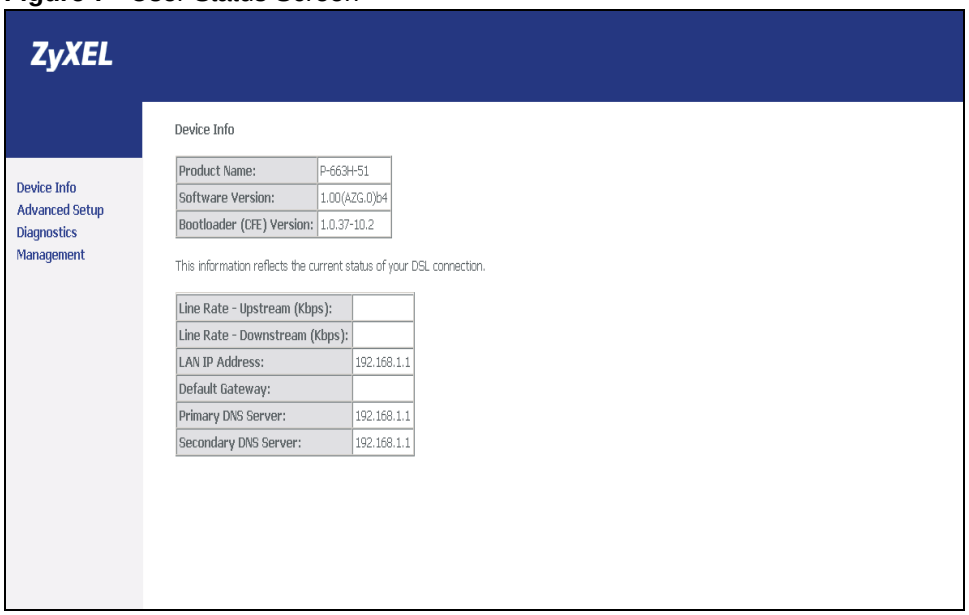
Figure 6 Password Screen



2.2.1 User Access

The user account can only access the ZyXEL Device from the LAN. For user access, enter the user account's user name (**user**) and password (**1234** is the default) and click **OK** to view the status only. The following screen appears.

Figure 7 User Status Screen



2.2.2 Administrator Access

The **admin** account can only access the ZyXEL Device from the LAN.

For administrator access, enter the administrator user name (**admin**) and password (**1234** is the default) and click **OK** to enter the configuration screens.

The management session automatically times out if it is left idle for five minutes. Simply log back into the ZyXEL Device if this happens.

2.3 Resetting the ZyXEL Device

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the ZyXEL Device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

2.3.1 Using the Reset Button

1. Make sure the **POWER** LED is on (not blinking).
2. Press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts.

2.4 Navigating the Web Configurator

After you log in, use the sub-menus on the navigation panel to go to other screens. Some fields or links are not available if you entered the user password in the login password screen (see Figure 7 on page 32).

Figure 8 Web Configurator: First Screen

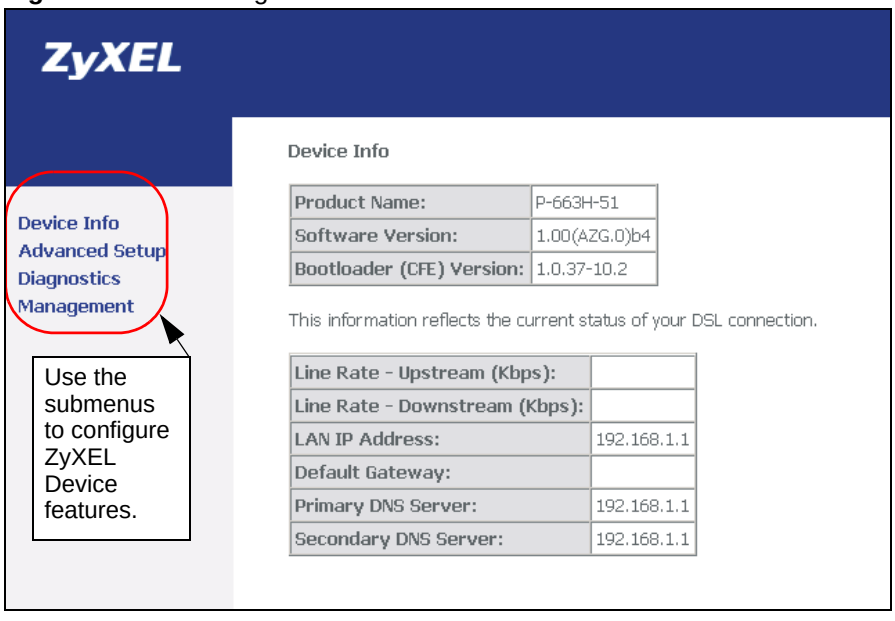


Table 2 Web Configurator Screens Summary

LINK/ICON	SUB-LINK	FUNCTION
Device Info		
Summary		This screen shows general device information such as the firmware version, line rates, LAN IP address, default gateway, and DNS servers.
WAN		This screen displays information about the ZyXEL Device's WAN connections.
Statistics	LAN	This screen displays statistics about the ZyXEL Device's LAN connections.
	WAN	This screen displays statistics about the ZyXEL Device's WAN connections.
	ATM	This screen shows low-level ATM protocol statistics.
	ADSL	This screen displays statistics about the ZyXEL Device's ADSL connection.
Route		This screen displays information about the ZyXEL Device's routes for sending traffic.
ARP		This screen displays the IP addresses and MAC addresses that the ZyXEL Device has resolved.
DHCP		This screen lists the ZyXEL Device's DHCP clients.
Advanced Setup		
WAN		Use these screens to view and configure the ZyXEL Device's WAN (Internet) connection settings.
LAN		Use this screen to configure LAN settings and the DHCP server.
NAT	Virtual Servers	Use this screen to configure NAT virtual server (port forwarding) entries to have the ZyXEL Device forward traffic from the WAN to LAN computers.
	Port Triggering	Use this screen to change your ZyXEL Device's port triggering settings.
	DMZ Host	Use this screen to configure a DMZ host IP address to receive packets from ports that are not specified in the virtual server configuration.
Security	IP Filtering	Configure outgoing IP filtering to block LAN users or applications from accessing the Internet. Configure incoming IP filtering to allow certain traffic to come in from the Internet to the LAN.
	MAC Filtering	Configure the MAC filter to block or allow access based on MAC addresses.
	Parental Control	Configure days and times to block Internet access from specific MAC addresses.
Quality of Service		Use the first QoS screen to enable or disable QoS, and select a DSCP mark to use on all outgoing packets that do not match a QoS classification rule.
	Queue Config	This screen lists the QoS queues. A QoS queue sets the priority used for incoming packets that the QoS classifier has grouped into a flow.
	QoS Classifications	Configure QoS classifiers to group upstream traffic into data flows according to specific criteria.

Table 2 Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
Routing	Default Gateway	Set the default gateway that helps the ZyXEL Device forward traffic to its destination.
	Static Route	Configure static routes to have the ZyXEL Device send data to devices not reachable through the default gateway.
	RIP	Configure RIP settings to have the ZyXEL Device exchange routing information with other routers.
DNS	DNS Server	Set how the ZyXEL Device selects a DNS server (for mapping domain names to IP addresses).
	Dynamic DNS	A dynamic DNS service lets the ZyXEL Device use a Web name like *.yourhost.dyndns.org while using a dynamic IP address. This lets others access the ZyXEL Device from the Internet without knowing it's IP address.
DSL		Use this screen to configure the ZyXEL Device's DSL settings.
Port Mapping		Use this screen to map ports to PVCs and create bridging groups.
Diagnostics		Use this screen to test the connections to your LAN devices (Ethernet connections) and your ADSL connection.
Management		
Settings	Backup	Use this screen to save the ZyXEL Device's configuration to a computer.
	Update	Use this screen to save a previously saved configuration file from a computer to the ZyXEL Device.
	Restore Default	Use this screen to reset the factory defaults to your ZyXEL Device.
System Log	View System Log	Use this screen to display the logs.
	Configure System Log	Use this screen to change your ZyXEL Device's log settings.
SNMP Agent		Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
Internet Time		Use this screen to configure how the ZyXEL Device synchronizes its internal clock with a time server on the Internet.
Access Control	Services	Use this screen to enable or disable service access to the ZyXEL Device.
	IP Addresses	Use these screens to configure the IP addresses of trusted computers that may manage the ZyXEL Device.
	Passwords	Use this screen to change the passwords for the ZyXEL Device's accounts.
Update Software		Use this screen to upload firmware to your ZyXEL Device.
Save/Reboot		Use this screen to save all of your ZyXEL Device's settings and reboot the ZyXEL Device without turning the power off.
Logout		Exit the web configurator.

Click **Management > Logout** to exit the web configurator.

3

Initial Configuration

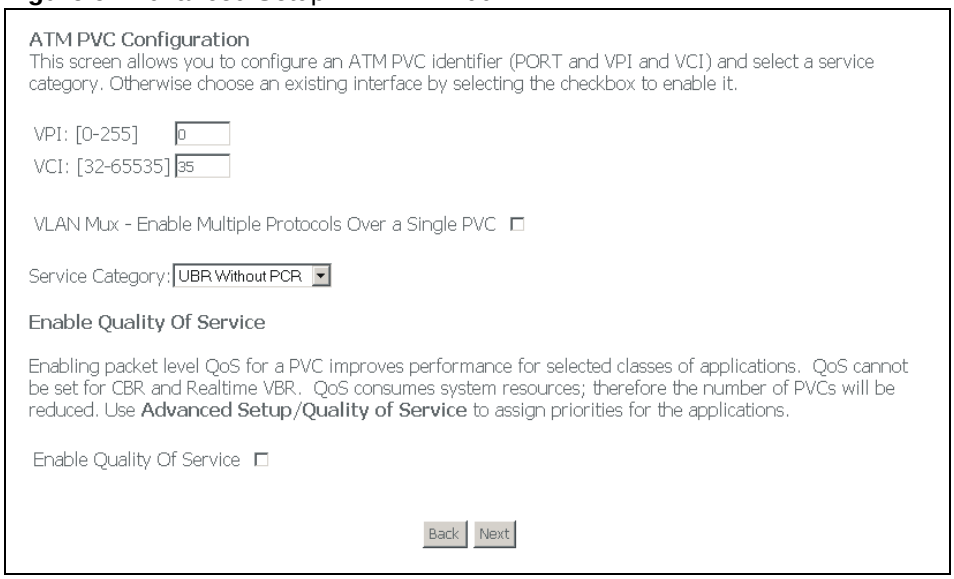
This chapter introduces the initial configuration that you may need to perform on the ZyXEL Device.

3.1 WAN Configuration

If you connect your ZyXEL Device and are able to access the Internet without configuring the ZyXEL Device, it may be that your ISP pre-configured the ZyXEL Device for you or the Internet connection works with the ZyXEL Device's default settings.

If you connect the ZyXEL Device and are not able to access the Internet, the ISP (Internet Service Provider) should have given you Internet connection information. This includes the connection type, VPI, VCI, and any values specific to your connection type (such as a user name and password). Click **Advanced Setup** > **WAN** > **Add** (or **Edit**). Use the following screen (and the ones that come after it) to configure your Internet connection. See Chapter 5 on page 51 for more information.

Figure 9 Advanced Setup > WAN > Add


ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Back
Next

3.2 QoS Configuration

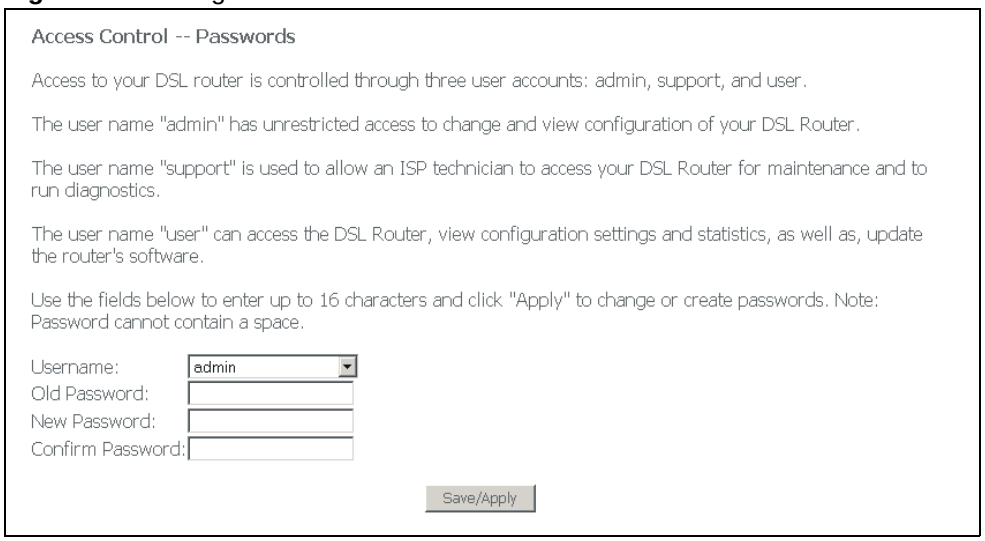
If the ISP gave you QoS settings to use, click **Advanced Setup** > **QoS** and configure the ZyXEL Device to use them. See Chapter 9 on page 89 for details.

If the WAN connection uses VLAN multiplexing, you can apply different QoS settings to different VLANs within the same WAN connection. If you are not using VLAN multiplexing, you may need to configure separate WAN connections (using different PVCs) in order to give different traffic different priorities.

3.3 Changing the Login Password

It is highly recommended that you periodically change the password for accessing the ZyXEL Device. Click **Management** > **Access Control** > **Passwords** to display the screen shown next. Use this screen to change the password. See Section 21.5 on page 135 for details.

Figure 10 Management > Access Control > Passwords


Access Control -- Passwords
Access to your DSL router is controlled through three user accounts: admin, support, and user.
The user name "admin" has unrestricted access to change and view configuration of your DSL Router.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
Username:
admin
Old Password:
New Password:
Confirm Password:
Save/Apply

4

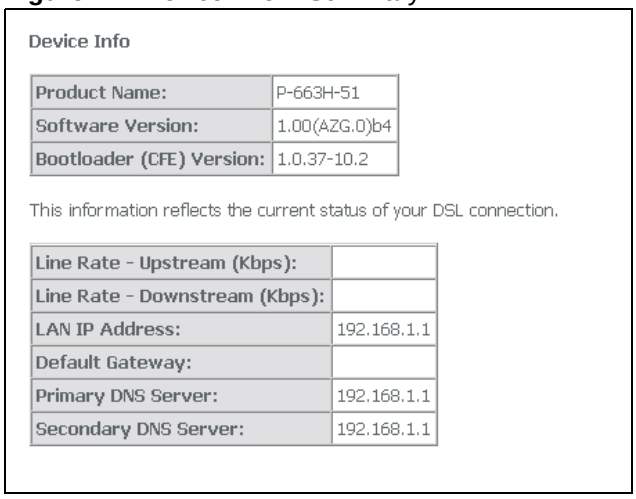
Device Information

Use the **Device Info** screens to see information about your ZyXEL Device and its connections.

4.1 Device Information Summary

The **Device Info** > **Summary** screen displays when you log in. To get to it from another screen, just click **Device Info** > **Summary**. This screen displays general information about the ZyXEL Device.

Figure 11 Device Info > Summary


Device Info
Product Name: P-663H-51
Software Version: 1.00(AZG.0)b4
Bootloader (CFE) Version: 1.0.37-10.2
This information reflects the current status of your DSL connection.
Line Rate - Upstream (Kbps):
Line Rate - Downstream (Kbps):
LAN IP Address: 192.168.1.1
Default Gateway:
Primary DNS Server: 192.168.1.1
Secondary DNS Server: 192.168.1.1

The following table describes the labels shown in the **Status** screen.

Table 3 Device Info > Summary

LABEL	DESCRIPTION
Product Name	This is your ZyXEL Device's model name.
Software Version	This is the number of the firmware release the ZyXEL Device is using.
Bootloader (CFE) Version	This is the number of the bootloader the ZyXEL Device is using.
Line Rate - Upstream (Kbps)	This is the speed of the upstream (outgoing) connection link.
Line Rate - Downstream (Kbps)	This is the speed of the downstream (incoming) connection link.
LAN IP Address	This is the IP address of the LAN ports.
Default Gateway	This is the IP address of the default gateway, if applicable.

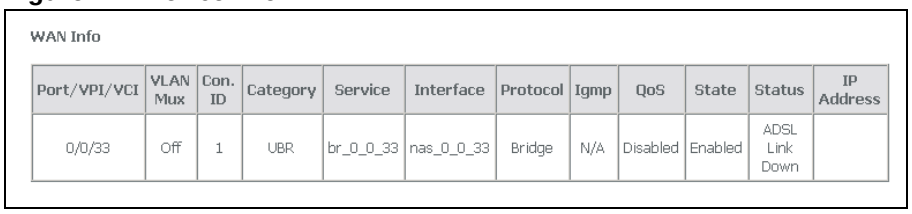
Table 3 Device Info > Summary

LABEL	DESCRIPTION
Primary DNS Server	This is the IP address of the server that the ZyXEL Device tries to use first when it needs to resolve a domain name (find the numeric IP address associated with the domain name).
Secondary DNS Server	If the primary server does not respond when the ZyXEL Device tries to resolve a domain name, the ZyXEL Device tries the server displayed in this field.

4.2 WAN Information

Click **Device Info** > **WAN** to open the following screen. Each row in the table displays information about one of the ZyXEL Device's WAN connections.

Figure 12 Device Info > WAN


WAN Info

Port/VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address
0/0/33	Off	1	UBR	br_0_0_33	nas_0_0_33	Bridge	N/A	Disabled	Enabled	ADSL Link Down	

The following table describes the labels in this screen.

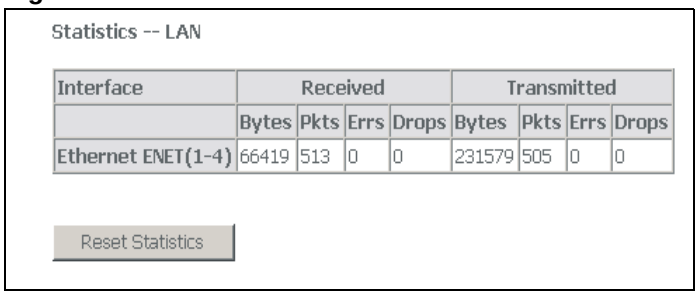
Table 4 Device Info > WAN

LABEL	DESCRIPTION
Port/VPI/VCI	This field displays the WAN connection's DSL port, Virtual Path Identifier, and Virtual Channel Identifier. The DSL port is always 0 because the DSL ports are bonded into a single logical port.
VLAN Mux.	This field shows whether or not VLAN multiplexing is enabled. VLAN multiplexing allows multiple separate WAN connections within the same PVC.
Con. ID	This is the number of the WAN connection.
Category	This is the ATM traffic class the WAN connection is using.
Service	This displays the connection type, DSL port, Virtual Path Identifier, and Virtual Channel Identifier. For the connection types, pppoe stands for PPPoE, ipoa stands for IPoA, pppoa stands for PPPoA, mer stands for MAC Encapsulated Routing, and br stands for bridging.
Interface	This field displays the name of the WAN connection, followed by the DSL port, Virtual Path Identifier, and Virtual Channel Identifier.
Protocol	This is the type of network protocol the WAN interface is using for IP over Ethernet.
IGMP	This is whether or not the WAN connection is using IGMP multicast (if available).
QoS	This is whether or not packet level QoS is enabled for the WAN connection.
State	This is whether or the WAN connection is enabled.
Status	This is the WAN connection's current ADSL line state.
IP Address	This is the WAN connection's IP address.

4.3 LAN Statistics

Click **Device Info** > **Statistics** > **LAN** to open the following screen. This screen displays statistics about the ZyXEL Device's LAN connections.

Figure 13 Device Info > Statistics > LAN



The following table describes the labels in this screen.

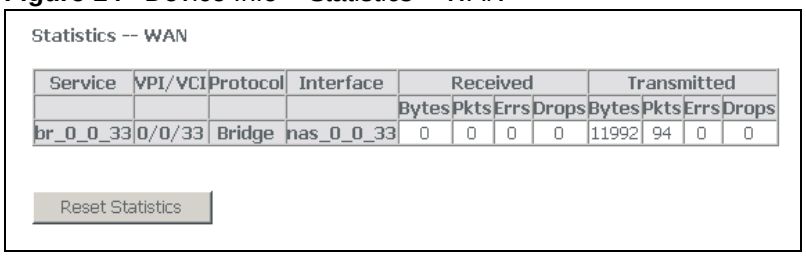
Table 5 Device Info > Statistics > LAN

LABEL	DESCRIPTION
Interface	This field displays the name of the port.
Received	These statistics are for traffic the ZyXEL Device has received on the LAN Ethernet interface.
Transmitted	These statistics are for traffic the ZyXEL Device has sent through the LAN Ethernet interface.
Bytes	This field displays the number of bytes received or sent.
Pkts	This field displays the number of packets received on or sent through the LAN port.
Errs	This field displays the number of error packets received on or sent through the LAN port.
Drops	This field displays the number of incoming or outgoing packets dropped.
Reset Statistics	Click this button to have the ZyXEL Device clear the current Ethernet statistics and start collecting them again.

4.4 WAN Statistics

Click **Device Info** > **Statistics** > **WAN** to open the following screen. Each row in the table displays statistics about a WAN connection.

Figure 14 Device Info > Statistics > WAN



The following table describes the labels in this screen.

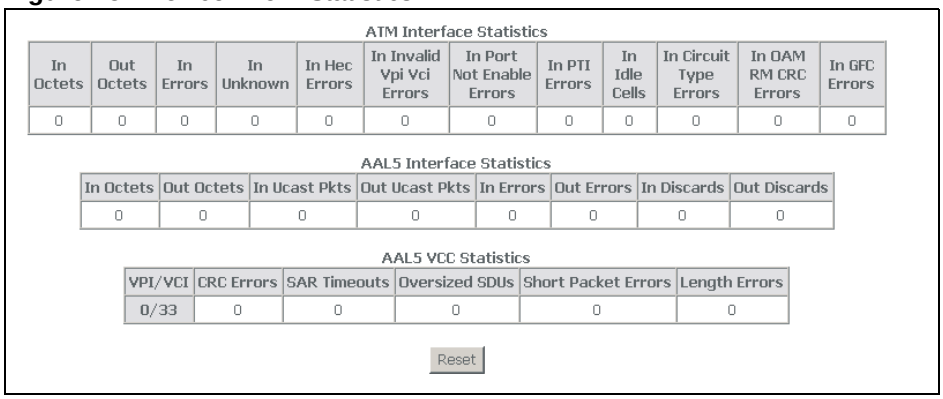
Table 6 Device Info > Statistics > WAN

LABEL	DESCRIPTION
Service	If the WAN connection is using bridging, the name of the bridge displays here.
VPI/VCI	This field displays the WAN connection's Virtual Path Identifier, and Virtual Channel Identifier.
Protocol	This is the type of network protocol the WAN interface is using for IP over Ethernet.
Interface	This field displays the name of the WAN connection.
Received	These statistics are for traffic the ZyXEL Device has received on the WAN connection.
Transmitted	These statistics are for traffic the ZyXEL Device has sent through the WAN connection.
Bytes	This field displays the number of bytes received or sent.
Pkts	This field displays the number of packets received on or sent through the WAN connection.
Errs	This field displays the number of error packets received on or sent through the WAN connection.
Drops	This field displays the number of incoming or outgoing packets dropped.
Reset Statistics	Click this button to have the ZyXEL Device clear the current WAN statistics and start collecting them again.

4.5 ATM Statistics

Click **Device Info** > **Statistics** > **ATM** to open the following screen. This screen shows low-level ATM protocol statistics.

Figure 15 Device Info > Statistics > ATM



The following table describes the labels in this screen.

Table 7 Device Info > Statistics > ATM

LABEL	DESCRIPTION
ATM Interface Statistics	These are statistics for the ATM interface.
In Octets	How many octets the interface received.
Out Octets	How many octets the interface transmitted.

Table 7 Device Info > Statistics > ATM (continued)

LABEL	DESCRIPTION
In Errors	How many cells the ZyXEL Device dropped because of uncorrectable HEC errors.
In Unknown	How many received cells the ZyXEL Device discarded during cell header validation. This includes cells with invalid cell header patterns or unrecognized VPI/VCI values. If the ZyXEL Device is set to discard cells with undefined PTI values, they are also included in this count.
In Hec Errors	How many cells the ZyXEL Device received with HEC errors in the ATM cell headers.
In Invalid Vpi Vci Errors	How many cells the ZyXEL Device received with an unregistered VCC (Virtual Channel Connection) address.
In Port Not Enable Errors	How many cells the ZyXEL Device received on disabled ports.
In PTI Errors	How many cells the ZyXEL Device received with an ATM header that had a Payload Type Indicator (PTI).
In Idle Cells	How many idle cells the ZyXEL Device received.
In Circuit Type Errors	How many idle cells the ZyXEL Device received with illegal circuit types.
In OAM RM CRC Errors	How many Operational, Administration and Maintenance Function 5 (OAM) and RM (Rate Management) cells the ZyXEL Device received with a Cyclic Redundancy Check error.
In GFC Errors	How many cells the ZyXEL Device received with non-zero GFCs.
AAL5 Interface Statistics	These are statistics for the AAL5 interface.
In Octets	How many AAL5/AAL0 CPCS PDU octets the ZyXEL Device received.
Out Octets	How many AAL5/AAL0 CPCS PDU octets the ZyXEL Device transmitted.
In Ucast Pkts	How many received AAL5/AAL0 CPCS PDUs the ZyXEL Device passed to higher layers.
Out Ucast Pkts	How many AAL5/AAL0 CPCS PDUs the ZyXEL Device received for transmission from higher layers.
In Errors	How many AAL5/AAL0 CPCS PDUs the ZyXEL Device received that contained errors. Including CRC-32 errors, SAR timeouts, and oversised SDUs.
Out Errors	How many AAL5/AAL0 CPCS PDUs the ZyXEL Device could not transmit due to errors.
In Discards	How many AAL5/AAL0 CPCS PDUs the ZyXEL Device discarded due to input buffer overflows.
Out Discards	How many non-errored AAL5/AAL0 CPCS PDUs the ZyXEL Device discarded. (For example, the ZyXEL Device might do this to free up buffer space.)
AAL5 VCC Statistics	These are statistics for the ATM VCC (Virtual Channel Connection) interface.
VPI/VCI	A VCC (Virtual Channel Connection) is a VPI and VCI combination. Each row in this table represents a VCC. This field displays the Virtual Path Identifier, and Virtual Channel Identifier of each VCC.
CRC Errors	How many PDUs the ZyXEL Device received on the VCC with CRC-32 errors.
SAR Timeouts	How many partially-reassembled PDUs the ZyXEL Device discarded because they were not fully reassembled during the allotted time period. This value is zero if the re-assembly timer is not supported.
Oversized SDUs	How many PDUs with corresponding SDUs that were too large (so the ZyXEL Device discarded them).

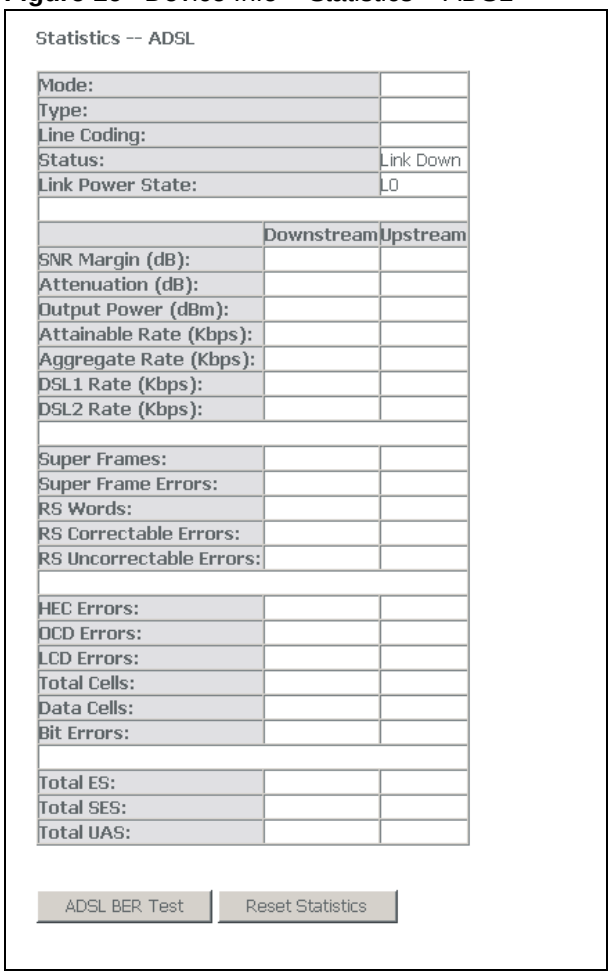
Table 7 Device Info > Statistics > ATM (continued)

LABEL	DESCRIPTION
Short Packet Errors	How many PDUs that had a length shorter than the size of the AAL5 trailer (so the ZyXEL Device discarded them).
Length Errors	How many PDUs the ZyXEL Device discarded because the length in the AAL5 trailer did not match the PDU length.
Reset Statisitcs	Click this button to have the ZyXEL Device clear the current ATM statistics and start collecting them again.

4.6 ADSL Statistics

Click **Device Info** > **Statistics** > **ADSL** to open the following screen. This screen displays statistics about the ZyXEL Device's ADSL connection.

Figure 16 Device Info > Statistics > ADSL



The following table describes the labels in this screen.

Table 8 Device Info > Statistics > ADSL

LABEL	DESCRIPTION
Mode	This is the ADSL mode that the ADSL link is using.
Type	
Line Coding	This shows whether the ADSL link is using Trellis coding or Reed-Solomon error correction. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable. “RS” coding stands for Reed-Solomon error correction.
Status	This shows the ADSL link’s connection status.
Link Power State	This is the ADSL connection’s current power management mode.
SNR Margin (dB)	This is the upstream and downstream Signal-to-Noise Ratio Margin (in dB). A DMT sub-carrier’s SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the ZyXEL Device still being able to meet its transmission targets.
Attenuation (dB)	This is the downstream and upstream Line Attenuation (in dB).
Output Power (dBm)	This field displays the amount of power being used to transmit to the other end of the ADSL link. Output power varies with the line length and quality. The longer the line is or the more interference there is on the line, the more power is needed.
Attainable Rate (Kbps)	These are the downstream and upstream highest theoretically possible transfer rates (in Kbps).
Aggregate Rate (Kbps)	These are the combined downstream and upstream rates (in Kbps) of the two DSL ports.
DSL1 Rate (Kbps)	These are the downstream and upstream rates (in Kbps) at which the DSL1 port has been receiving and sending data.
DSL2 Rate (Kbps)	These are the downstream and upstream rates (in Kbps) at which the DSL2 port has been receiving and sending data.
Super Frames	These are the downstream and upstream numbers of downstream and upstream super frames.
Super Frame Errors	These are the downstream and upstream numbers of errored super frames sent and received.
RS Words	These are the downstream and upstream numbers of Reed-Solomon error correction words.
RS Correctable Errors	These are the downstream and upstream numbers of Reed-Solomon errors.
RS Uncorrectable Errors	The number of downstream and upstream uncorrectable Reed-Solomon errors.
HEC Errors	These are the downstream and upstream numbers of Header Error Control errors.
OCD Errors	These are the downstream and upstream numbers of Out of Cell Delineation errors.
LCD Errors	The number of 1-second intervals since reset where loss of cell delineation occurred.
Total Cells	The total numbers of downstream and upstream ATM cells.
Data Cells	The total numbers of downstream and upstream data cells.
Bit Errors	The total numbers of downstream and upstream bit errors.

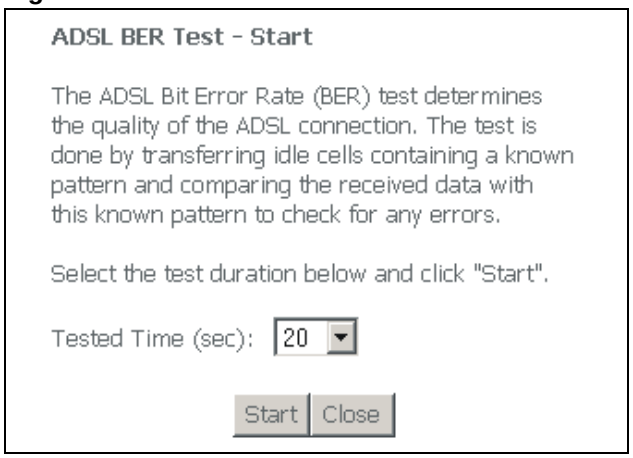
Table 8 Device Info > Statistics > ADSL (continued)

LABEL	DESCRIPTION
Total ES	The number of Errored SecondS that have occurred within the period.
Total SES	The number of Severely Errored Seconds that have occurred within the period.
Total UAS	The number of UnAvailable Seconds that have occurred within the period.
ADSL BER Test	Click this button to perform an ADSL Bit Error Rate Test to measure the quality of the ADSL connection.
Reset Statisitcs	Click this button to have the ZyXEL Device clear the current ADSL statistics and start collecting them again.

4.7 ADSL BER Test

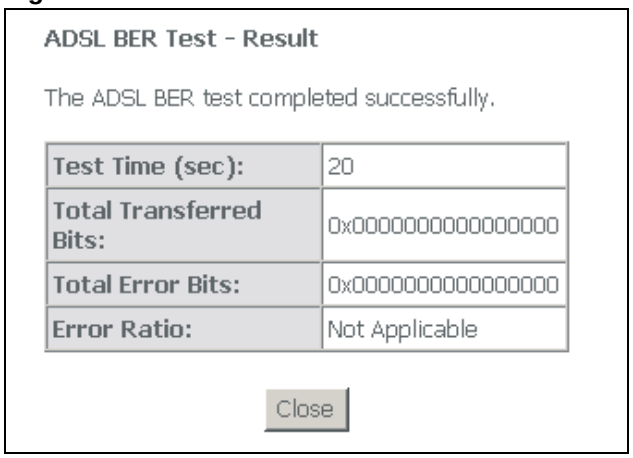
Click **Device Info** > **Statistics** > **ADSL** > **ADSL BER Test** to open the following screen. Perform an ADSL Bit Error Rate Test to measure the quality of the ADSL connection.

Figure 17 Device Info > Statistics > ADSL > ADSL BER Test


ADSL BER Test - Start
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 20
Start
Close

Select for how many seconds to perform the test and click **Start**.

Figure 18 Device Info > Statistics > ADSL > ADSL BER Test: Results


ADSL BER Test - Result
The ADSL BER test completed successfully.
Test Time (sec): 20
Total Transferred Bits: 0x0000000000000000
Total Error Bits: 0x0000000000000000
Error Ratio: Not Applicable
Close

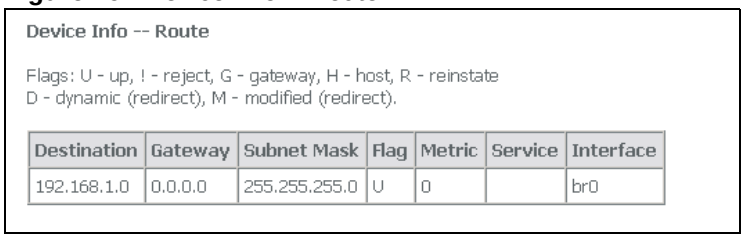
The ADSL BER test results show how many bits were sent, how many of the transferred bits were errored, and the error ratio.

Click **Close** when you are done.

4.8 Route Info

Click **Device Info** > **Route** to open the following screen. This screen displays information about the ZyXEL Device's routes for sending traffic.

Figure 19 Device Info > Route



The following table describes the labels in this screen.

Table 9 Device Info > Route

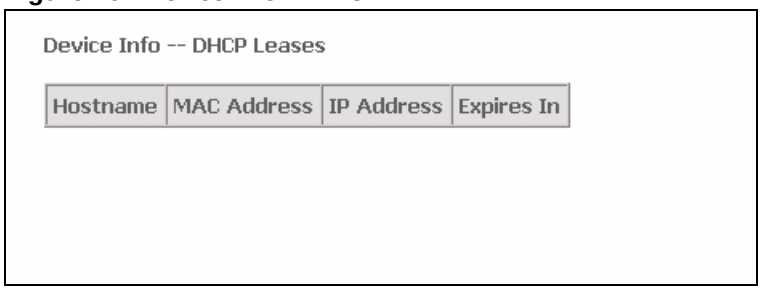
LABEL	DESCRIPTION
Destination	The route applies to traffic going to this network address.
Gateway	This is the router the ZyXEL Device sends traffic to in order to forward the traffic to the destination listed in the route.
Subnet Mask	This is the network number of the gateway to which this route forwards traffic.
Flag	This displays more information about the route. U - up ! -reject G - gateway H - host R - reinstate D - dynamic (redirect) M - modified (redirect)
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Service	This displays what type of traffic this route is for. The field is blank when the route is for all types of service.
Interface	This route has the ZyXEL Device send traffic through this interface.

4.8.1 DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If DHCP service is disabled, there must be another DHCP server, or else the computer must be manually configured.

Click **Device Info** > **DHCP** to display the following screen. This is only available when the ZyXEL Device's DHCP server function is enabled. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyXEL Device's DHCP server.

Figure 20 Device Info > DHCP



The following table describes the labels in this screen.

Table 10 Device Info > DHCP

LABEL	DESCRIPTION
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address assigned to the DHCP client.
Expires	This field displays for how much longer the host has the lease for the assigned IP address.

PART II
Advanced

WAN Setup (51)
LAN Setup (67)
Network Address Translation (NAT) Screens (73)
Security (81)
Quality of Service (QoS) (89)
Routing (97)
RIP (101)
DNS Setup (103)
Dynamic DNS Setup (105)
DSL Setup (109)
Port Mapping (111)

5

WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

5.1.1 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

5.1.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

5.1.2.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

5.1.2.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

5.2 Traffic Shaping

Traffic shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Note: Traffic shaping controls outgoing (upstream) traffic, not incoming (downstream).

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

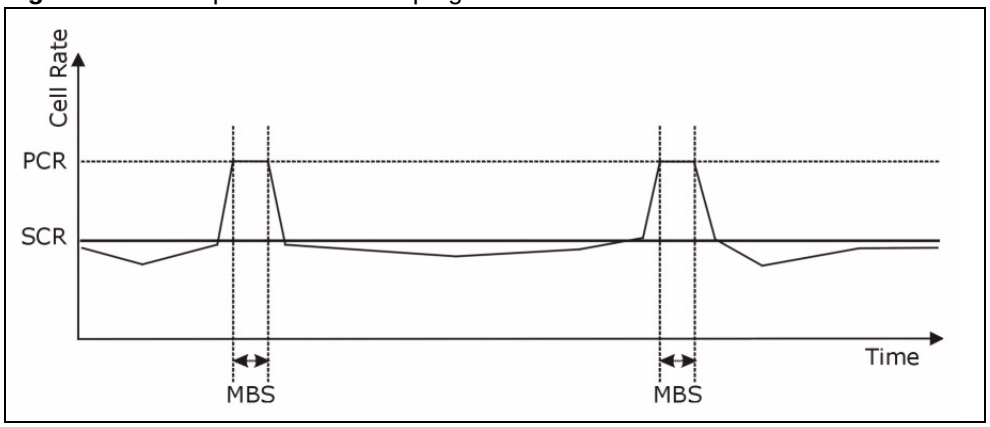
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 21 Example of Traffic Shaping



5.2.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

5.2.1.1 Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

5.2.1.2 Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into realtime or non realtime connections.

The realtime VBR type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an realtime VBR connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The non realtime VBR type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an non realtime VBR connection would be non-time sensitive data file transfers.

5.2.1.3 Unspecified Bit Rate (UBR)

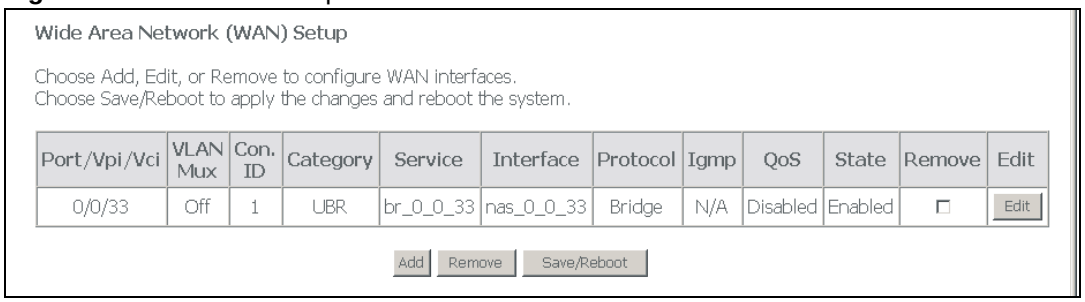
The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

5.3 WAN

Click **Advanced Setup** > **WAN** to open the following screen. This screen displays your ZyXEL Device's WAN Internet access settings. You can also edit those settings and add more settings. The screen differs by the encapsulation.

See Section 5.1 on page 51 for more information.

Figure 22 Advanced Setup > WAN



The following table describes the labels in this screen.

Table 11 Advanced Setup > WAN

LABEL	DESCRIPTION
Port/VPI/VCI	This field displays the WAN connection's DSL port, Virtual Path Identifier, and Virtual Channel Identifier. The DSL port is always 0 because the DSL ports are bonded into a single logical port.
VLAN Mux.	This field shows whether or not VLAN multiplexing is enabled. VLAN multiplexing allows multiple separate WAN connections within the same PVC.
Con. ID	This is the number of the WAN connection.
Category	This is the ATM traffic class the WAN connection is using.
Service	This displays the connection type, DSL port, Virtual Path Identifier, and Virtual Channel Identifier. For the connection types, pppoe stands for PPPoE, ipoa stands for IPoA, pppoa stands for PPPoA, mer stands for MAC Encapsulated Routing, and br stands for bridging.

Table 11 Advanced Setup > WAN (continued)

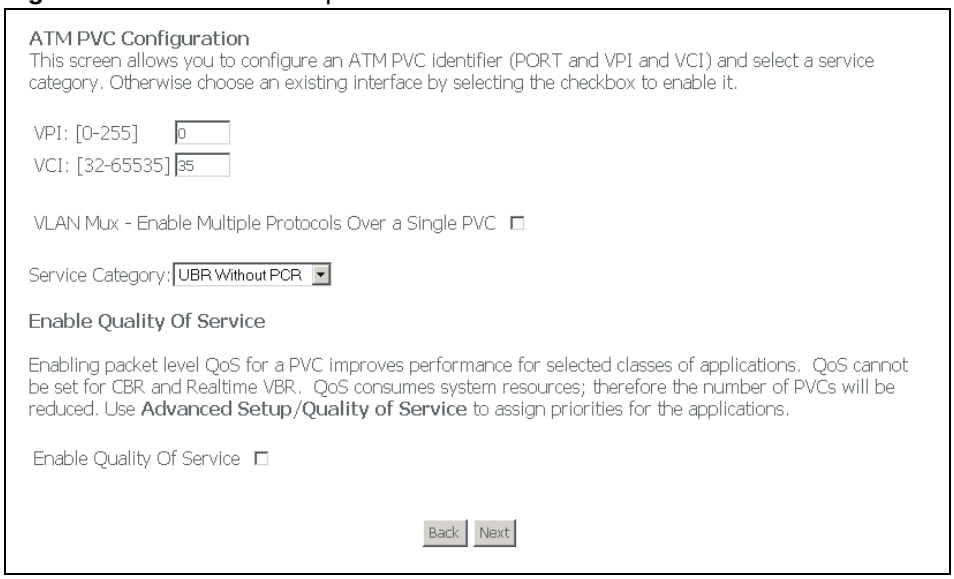
LABEL	DESCRIPTION
Interface	This field displays the name of the WAN connection, followed by the DSL port, Virtual Path Identifier, and Virtual Channel Identifier.
Protocol	This is the type of network protocol the WAN interface is using for IP over Ethernet.
IGMP	This is whether or not the WAN connection is using IGMP multicast (if available).
QoS	This is whether or not packet level QoS is enabled for the WAN connection.
State	This is whether or the WAN connection is enabled.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.
Edit	Click this button to go to a screen where you can modify the WAN connections settings.
Add	Click this button to go to a screen where you can configure settings for a new WAN connection.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.
Save/Reboot	Click this button to apply and save your changes. The ZyXEL Device restarts.

5.4 WAN ATM PVC Configuration and QoS

Click **Advanced Setup** > **WAN** > **Add** (or **Edit**) to open the following screen. Use this screen to configure ATM PVC settings and enable or disable QoS. The screen differs by the service category.

See Section 5.1 on page 51 for more information.

Figure 23 Advanced Setup > WAN > Add


ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Back
Next

The following table describes the labels in this screen.

Table 12 Advanced Setup > WAN > Add

LABEL	DESCRIPTION
ATM PVC Configuration	The PORT (interface), VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define an ATM PVC (Permanent Virtual Circuit). Refer to the appendix for more information.
VPI	Enter the VPI assigned to you for this WAN connection.
VCI	Enter the VCI assigned to you for this WAN connection.
VLAN Mux.	Select the check box to use VLAN multiplexing to allow multiple separate protocols to use the same PVC. Selecting this enables IEEE 802.1q. Separate VLANs can be used to give different priorities to the traffic from different ports.
802.1Q VLAN ID	When you enable VLAN multiplexing, type the VLAN ID that the ZyXEL Device is to add to the traffic sent through this WAN connection.
Service Category	Select **UBR** (unspecified bit rate) for applications that are non-time sensitive, such as e-mail. Use it with PCR if you want to specify a maximum rate at which the sender can send cells. Select **CBR** (constant bit rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Realtime VBR** for bursty traffic connections that require closely controlled delay and delay variation (like video conferencing). Use **Non Realtime VBR** for bursty connections that do not require closely controlled delay and delay variation (like non-time sensitive data file transfers).
Peak Cell Rate	The Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. PCR applies with all of the ATM traffic classes. Type a number of (ATM) cells per second (1~255000).
Sustainable Cell Rate	The Sustained Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. SCR applies with the **VBR** traffic classes. Type a number of (ATM) cells per second. The SCR must be less than the PCR.
Maximum Burst Size	The Maximum Burst Size (MBS) sets the maximum number of cells that the port should handle without any discards. Type the MBS here (1~1000000). MBS applies with the **VBR** traffic classes.
Enable Quality of Service	Enable the (packet level) QoS if you need to provide improved performance for certain classes of applications (like VoIP or video conferencing).
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.5 Connection Types

Be sure to use the connection type required by your ISP. Here is background information on the connection types the ZyXEL Device supports.

5.5.1 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

5.5.2 PPPoE

PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. The ZyXEL Device bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendices.

5.5.3 MER

MER (MAC Encapsulated Routing) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells.

5.5.4 IPoA

IPoA (Internet Protocol over ATM) in RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

5.5.5 Bridging

With bridging the ZyXEL Device has a static IP address for the connection. The ZyXEL Device passes traffic through to another device (a computer or router for example) that handles authenticating with the ISP.

5.6 Encapsulation

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the encapsulation method required by your ISP.

5.6.1 LLC-based Encapsulation

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

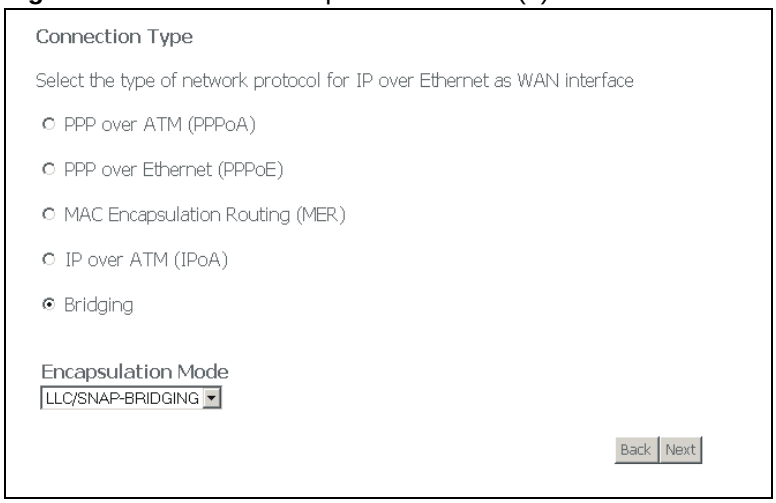
5.6.2 VC-based Encapsulation

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

5.7 WAN Connection Type and Encapsulation Mode

This is the second WAN setup add (or edit) screen. Use this screen to configure WAN connection type and encapsulation mode.

Figure 24 Advanced Setup > WAN > Add (2)



The following table describes the labels in this screen.

Table 13 Advanced Setup > WAN

LABEL	DESCRIPTION
Connection Type	Select the type of network protocol the ISP uses for IP over Ethernet.
Encapsulation Mode	Select the encapsulation mode that your ISP uses.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.8 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

5.9 Nailed-Up Connection (PPP)

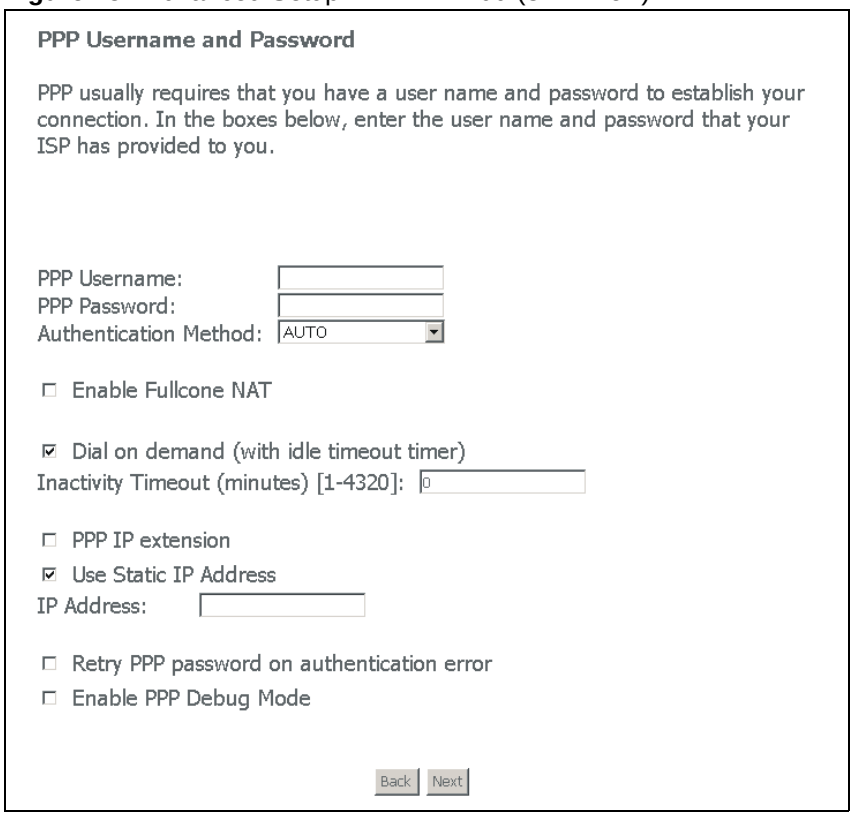
A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyXEL Device does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyXEL Device will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern

5.10 PPPoA WAN Connection Setup

When you select PPPoA in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure PPPoA connection settings.

Figure 25 Advanced Setup > WAN > Add (3: PPPoA)


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Authentication Method:
AUTO
Enable Fullcone NAT
Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]:
0
PPP IP extension
Use Static IP Address
IP Address:
Retry PPP password on authentication error
Enable PPP Debug Mode
Back
Next

The following table describes the labels in this screen.

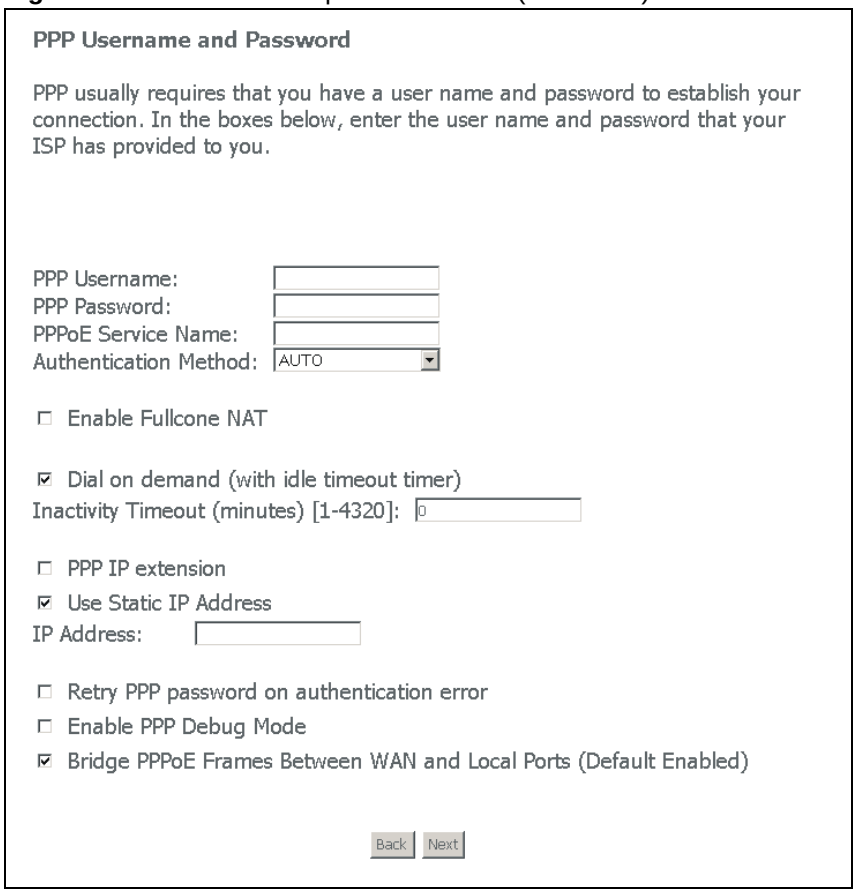
Table 14 Advanced Setup > WAN > Add (3: PPPoA)

LABEL	DESCRIPTION
PPP User Name	Enter the login name that your ISP gives you.
PPP Password	Enter the password associated with the user name above.
Authentication Method	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your ZyXEL Device accepts either CHAP, PAP, or MSCHAP when requested by this remote node. **CHAP** - Your ZyXEL Device accepts CHAP only. **PAP** - Your ZyXEL Device accepts PAP only. **MSCHAP** - Your ZyXEL Device accepts MSCHAP (Microsoft CHAP) only.
Enable Full Cone NAT	In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the ZyXEL Device.
Dial on demand	Select **Dial on demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Inactivity Timeout** field. Clear the **Dial on demand** option to keep the connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
PPP IP extension	Only select this option if your service provider requires it. The following conditions apply to a connection using PPP IP extension. • Only one computer can be connected on the LAN. • The ISP only assigns a single public IP address and the LAN computer uses it on its LAN interface. • The firewall and NAT features are disabled. • The ZyXEL Device uses DHCP to tell the LAN computer that the ZyXEL Device is its default gateway and DNS server. • The ZyXEL Device extends the ISP's IP subnet to the LAN computer. • The ZyXEL Device bridges packets between the DSL and LAN interface, except for packets destined for the ZyXEL Device's LAN IP address.
Use Static IP Address	If the ISP gave you a static (fixed) IP address, select this option and enter it in the **IP Address** field. If the ISP did not give you a static IP address, clear the **Use Static IP Address** option. The ISP automatically assigns the WAN connection an IP address when it connects.
Retry PPP password on authentication error	Select this to have the ZyXEL Device keep trying to connect using the password if there is an authentication error.
Enable PPP debug mode	Select this to turn on the debug mode for the PPP connection.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.11 PPPoE WAN Connection Setup

When you select PPPoE in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure PPPoE connection settings.

Figure 26 Advanced Setup > WAN > Add (3: PPPoE)


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method:
AUTO
Enable Fullcone NAT
Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]:
0
PPP IP extension
Use Static IP Address
IP Address:
Retry PPP password on authentication error
Enable PPP Debug Mode
Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)
Back
Next

The following table describes the labels in this screen.

Table 15 Advanced Setup > WAN > Add (3: PPPoE)

LABEL	DESCRIPTION
PPP User Name	Enter the login name that your ISP gives you.
PPP Password	Enter the password associated with the user name above.
Authentication Method	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your ZyXEL Device accepts either CHAP, PAP, or MSCHAP when requested by this remote node. **CHAP** - Your ZyXEL Device accepts CHAP only. **PAP** - Your ZyXEL Device accepts PAP only. **MSCHAP** - Your ZyXEL Device accepts MSCHAP (Microsoft CHAP) only.

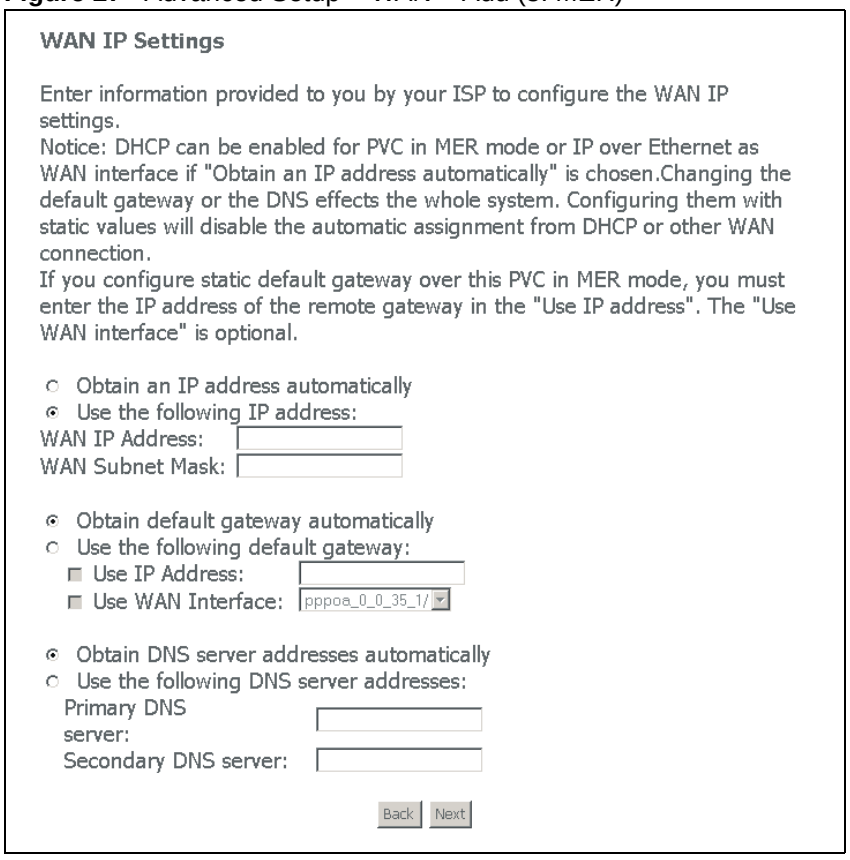
Table 15 Advanced Setup > WAN > Add (3: PPPoE) (continued)

LABEL	DESCRIPTION
Enable Full Cone NAT	In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the ZyXEL Device.
Dial on demand	Select **Dial on demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Inactivity Timeout** field. Clear the **Dial on demand** option to keep the connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
PPP IP extension	Only select this option if your service provider requires it. The following conditions apply to a connection using PPP IP extension. • Only one computer can be connected on the LAN. • The ISP only assigns a single public IP address and the LAN computer uses it on its LAN interface. • The firewall and NAT features are disabled. • The ZyXEL Device uses DHCP to tell the LAN computer that the ZyXEL Device is its default gateway and DNS server. • The ZyXEL Device extends the ISP's IP subnet to the LAN computer. • The ZyXEL Device bridges packets between the DSL and LAN interface, except for packets destined for the ZyXEL Device's LAN IP address.
Use Static IP Address	If the ISP gave you a static (fixed) IP address, select this option and enter it in the **IP Address** field. If the ISP did not give you a static IP address, clear the **Use Static IP Address** option. The ISP automatically assigns the WAN connection an IP address when it connects.
Retry PPP password on authentication error	Select this to have the ZyXEL Device keep trying to connect using the password if there is an authentication error.
Enable PPP debug mode	Select this to turn on the debug mode for the PPP connection.
Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)	This feature is available when you do not select **PPP IP extension**. In addition to the ZyXEL Device's built-in PPPoE client, you can enable this to pass PPPoE through in order to allow LAN hosts to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.12 MER WAN Connection Setup

When you select MER in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure MER connection settings.

Figure 27 Advanced Setup > WAN > Add (3: MER)


WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface:
pppoa_0_0_35_1/
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

The following table describes the labels in this screen.

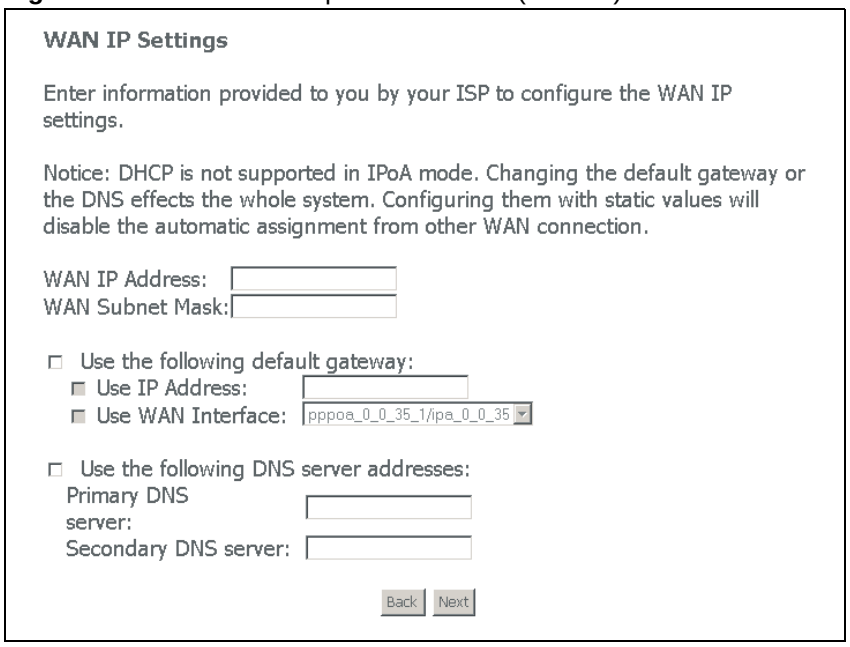
Table 16 Advanced Setup > WAN > Add (3: MER)

LABEL	DESCRIPTION
Obtain an IP address automatically	The WAN connection's IP address identifies the ZyXEL Device on the Internet. If the ISP did not give you a static IP address, select **Obtain an IP address automatically**. The ISP automatically assigns the WAN connection an IP address when it connects.
Use the following IP address	If the ISP gave you a static (fixed) IP address, select this option and enter the connection's IP address and subnet mask.
Obtain default gateway automatically	The default is a neighboring router that helps the ZyXEL Device forward traffic to its destination. If the ISP did not give you the IP address of the default gateway, select **Obtain default gateway automatically**. The ISP automatically assigns the WAN connection an IP address when it connects.
Use the following default gateway	Select this option to use a specific default gateway. Either enter the gateway's IP address or select the WAN interface to use to connect to it.
Obtain DNS server addresses automatically	The ZyXEL Device uses a DNS server to resolve a domain name (find the numeric IP address associated with the domain name). Select this option if the ISP did not give you a specific DNS server IP address. The ISP automatically assigns the DNS server IP addresses when the ZyXEL Device connects.
Use the following DNS server addresses	If the ISP gave you DNS server IP addresses, select this option and enter them in the fields below.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.13 IPoA WAN Connection Setup

When you select IPoA in the second WAN setup add (or edit) screen, this screen displays next. Use this screen to configure IPoA connection settings.

Figure 28 Advanced Setup > WAN > Add (3: IPoA)


WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.
WAN IP Address:
WAN Subnet Mask:
Use the following default gateway:
Use IP Address:
Use WAN Interface:
pppoa_0_0_35_1/ipa_0_0_35
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

The following table describes the labels in this screen.

Table 17 Advanced Setup > WAN > Add (3: IPoA)

LABEL	DESCRIPTION
WAN IP Address	Enter the IP address from the ISP. Use dotted decimal notation (like 192.168.1.1 for example).
WAN Subnet Mask	Enter the subnet mask from the ISP. Use dotted decimal notation (like 255.255.0.0 for example).
Use the following default gateway	The default is a neighboring router that helps the ZyXEL Device forward traffic to its destination. Select this option and enter the gateway's IP address or select the WAN interface to use to connect to it.
Use the following DNS server addresses	The ZyXEL Device uses a DNS server to resolve a domain name (find the numeric IP address associated with the domain name). Select this option. Enter the DNS server addresses from the ISP in the fields below.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.14 IGMP Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

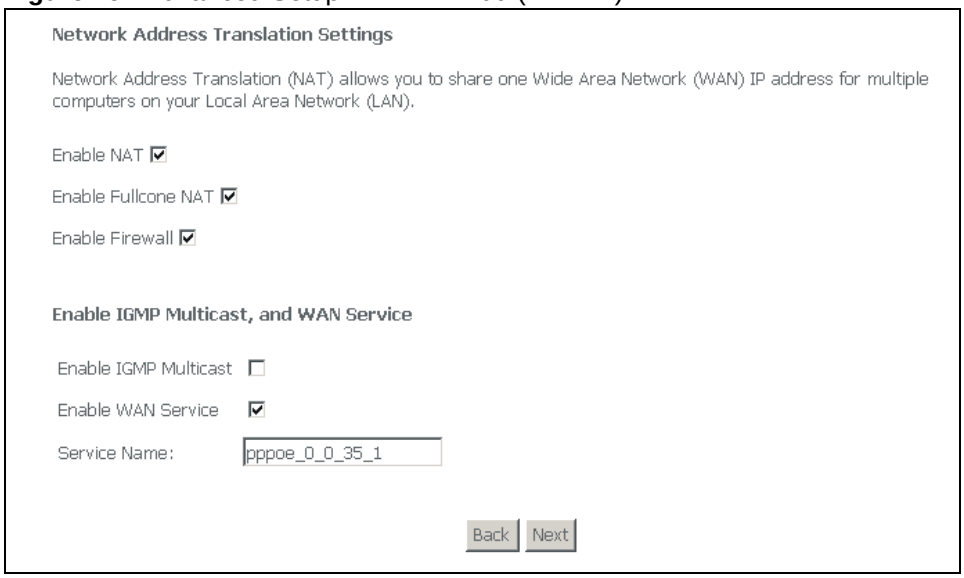
IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

5.15 NAT, IGMP Multicast, and WAN Service

This is the fourth WAN screen to display for every connection type except bridging (for which this is the third screen). This screen varies depending on the connection type. Use this screen to configure NAT, IGMP multicast, and WAN service settings.

Figure 29 Advanced Setup > WAN > Add (4: MER)


Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Fullcone NAT
Enable Firewall
Enable IGMP Multicast, and WAN Service
Enable IGMP Multicast
Enable WAN Service
Service Name:
pppoe_0_0_35_1
Back
Next

The following table describes the labels in this screen.

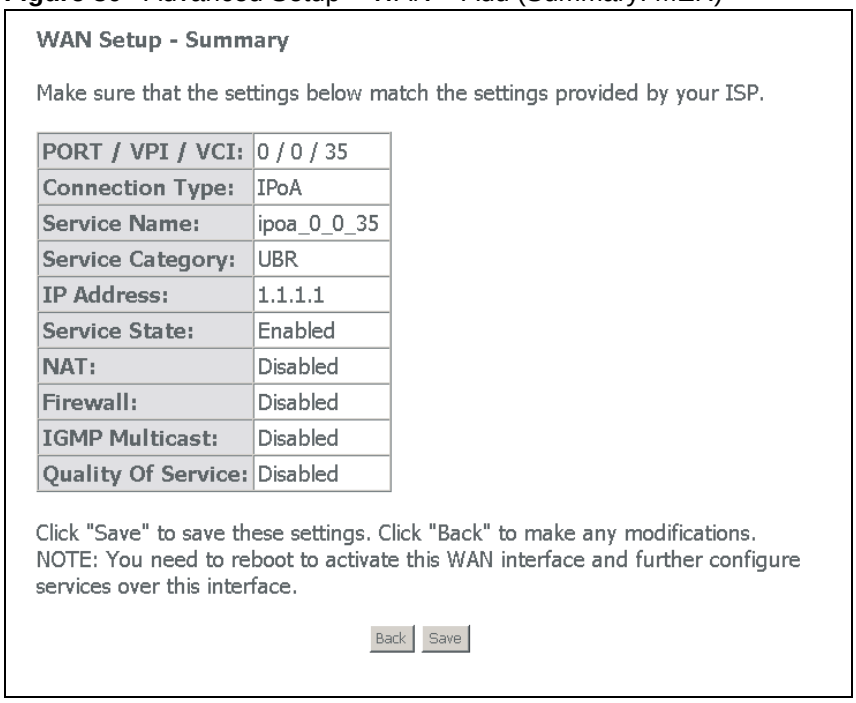
Table 18 Advanced Setup > WAN > Add (4: MER)

LABEL	DESCRIPTION
Enable NAT	Turn on NAT to translate IP addresses between two different networks (so you can have a private LAN with IP addresses that are different from the public IP addresses on the WAN. See Chapter 7 on page 73 for more details.
Enable Fullcone NAT	This field displays when you enable NAT. In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the ZyXEL Device. The ZyXEL Device uses restricted cone NAT when you disable full cone NAT.
Enable Firewall	Turn on the firewall to block traffic originating from the WAN from going to the LAN.
Enable IGMP Multicast	IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Turn this on to allow multicast traffic and have the ZyXEL Device act as an IGMP proxy.
Enable WAN Service	Select this option to use this WAN connection or clear the option to not use this WAN connection.
Service Name	This is the name for the WAN connection. Use the default or define your own.
Back	Click this to return to the previous screen.
Next	Click this to go to the following screen.

5.16 WAN Setup Summary

This is the last WAN setup screen to display. Use this screen to check your settings before saving them. Click **Back** if you need to make any changes. If the settings are OK, click **Save** to save the settings. Use the **Save/Reboot** button in the **Advanced Setup** > **WAN** screen to restart the ZyXEL Device and use the WAN connection settings.

Figure 30 Advanced Setup > WAN > Add (Summary: MER)



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_0_35
Service Category:	UBR
IP Address:	1.1.1.1
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

Back Save

6

LAN Setup

This chapter describes how to configure LAN settings.

6.1 LAN Overview

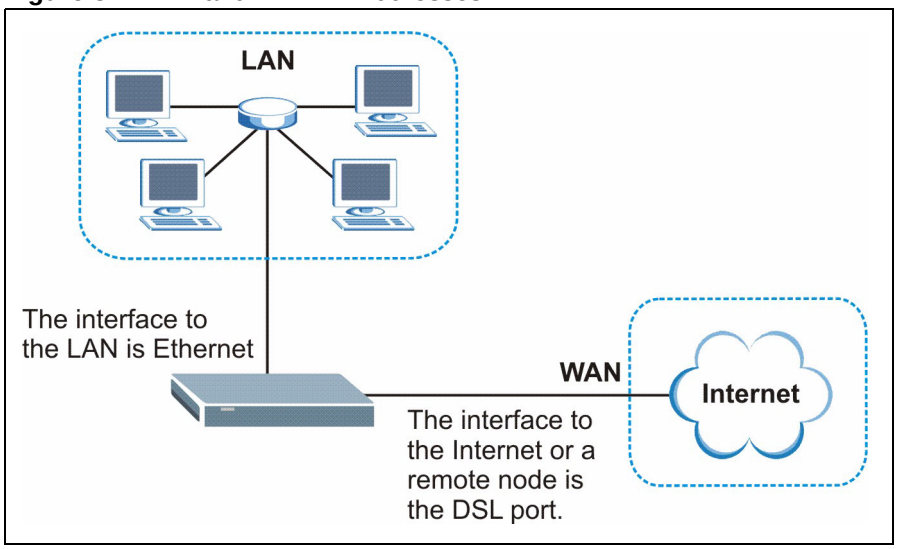
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See Section 6.5 on page 70 to configure the **LAN** screens.

6.1.1 LAN, WAN and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 31 LAN and WAN IP Addresses



6.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured. Do not assign static IP addresses from the DHCP pool to your LAN computers.

6.2 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

6.2.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

6.2.1.1 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255

- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

6.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

6.4 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

6.4.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

6.4.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

6.4.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages only on the LAN.

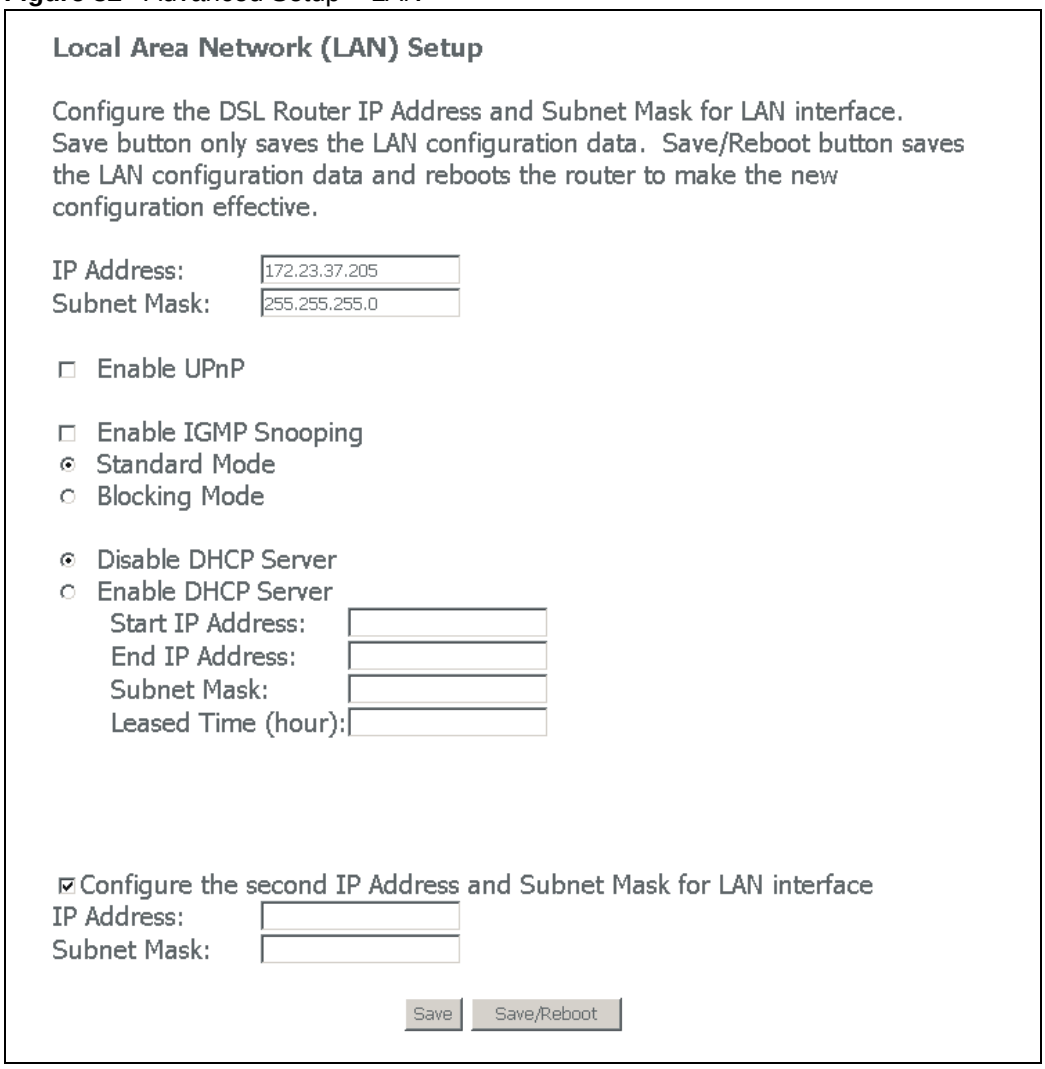
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

You must have IIS (Internet Information Services) enabled on the Windows web server for UPnP to work.

6.5 LAN Setup

Click **Advanced Setup** > **LAN** to open the **IP** screen. See Section 6.1 on page 67 for background information. Some fields may not display depending on your WAN configuration.

Figure 32 Advanced Setup > LAN



The following table describes the fields in this screen.

Table 19 Advanced Setup > LAN

LABEL	DESCRIPTION
IP Address	Enter the LAN IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask.
Enable UPnP	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Enable IGMP Snooping	Turn on IGMP snooping to reduce network traffic by having the ZyXEL Device only forward multicast traffic to ports connected to computers or devices that belong to the specific multicast group. Use standard mode to flood unknown multicast traffic. Use blocking mode to discard unknown multicast traffic.

Table 19 Advanced Setup > LAN (continued)

LABEL	DESCRIPTION
Disable/Enable DHCP Server	Turn on the DHCP server to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to DHCP clients on the LAN. Enter IP addresses in the **Start** and **End IP Address** fields to set a range of IP addresses for the ZyXEL Device to give to the DHCP clients. Enter an IP address in the **Start IP Address** field and a subnet mask in the **Subnet Mask** field to set a subnet of IP addresses for the ZyXEL Device to give to the DHCP clients. **Leased Time** sets how many hours to let a DHCP client use an IP before re-assigning it an IP address.
Configure the second IP address and subnet mask for LAN interface	Select this option to let the ZyXEL Device use a second IP address on the LAN interface. You can also use this second IP address to access the ZyXEL Device for management. Enter the LAN IP address of your ZyXEL Device in dotted decimal notation, for example, 10.0.0.1. Type the subnet mask.
Save	Click **Save** to save your changes to the ZyXEL Device.
Save/Reboot	Click this button to apply and save your changes. The ZyXEL Device restarts.

7

Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the ZyXEL Device.

7.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

7.2 NAT Virtual Servers

Configure NAT virtual server (port forwarding) entries to have the ZyXEL Device forward traffic from the WAN to LAN computers.

You might do this to get particular games or services to work through NAT. You can also make servers, for example, web or FTP, visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

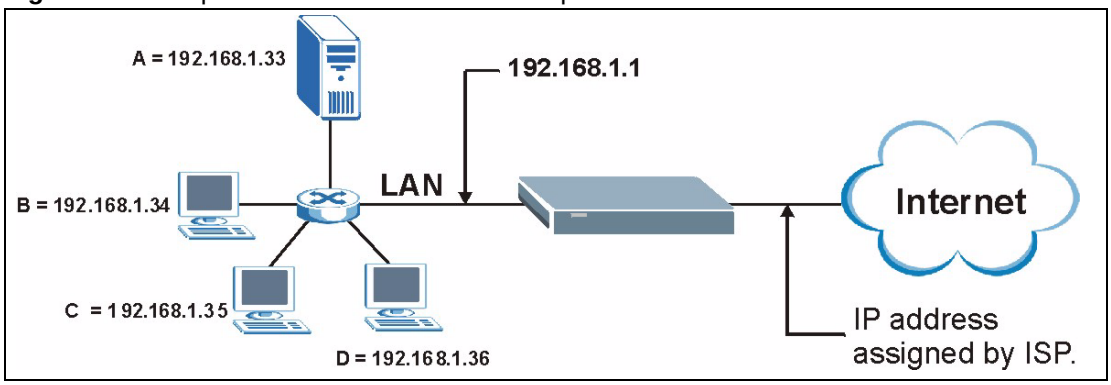
7.2.1 Virtual Server: Services and Port Numbers

See Appendix D on page 185 for commonly used port numbers.

7.2.2 Virtual Servers Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 33 Multiple Servers Behind NAT Example



7.3 Configuring Virtual Servers

The NAT screens are available only when you enable NAT in the WAN configuration.

Click **Advanced Setup** > **NAT** > **Virtual Servers** to open the following screen.

Figure 34 Advanced Setup > NAT > Virtual Servers

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
Diablo II	4000	4000	TCP	4000	4000	192.168.1.100	☐
Diablo II	6112	6119	UDP	6112	6119	192.168.1.100	☐

See Appendix D on page 185 for port numbers commonly used for particular services. The following table describes the fields in this screen.

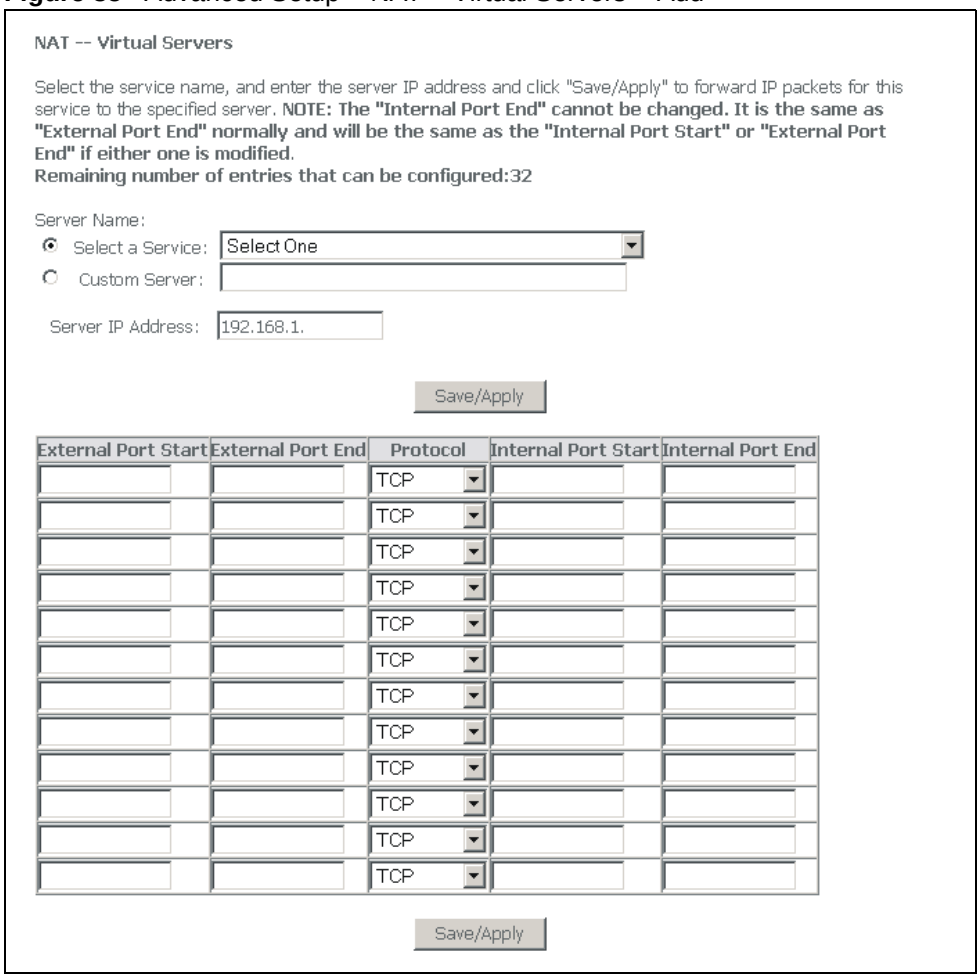
Table 20 NAT Port Forwarding

LABEL	DESCRIPTION
Add	Click this button to go to a screen where you can configure a new entry.
Remove	To remove an entry(ies), select its **Remove** check box and click the **Remove** button.
Server Name	This name identifies the virtual server entry.
External Port Start, External Port End	These are the ports of traffic coming in from the WAN to which this virtual server entry applies.
Protocol	This is the underlying protocol of the traffic to which this virtual server entry applies.
Internal Port Start, Internal Port End	These are the ports the ZyXEL Device uses for the traffic that it forwards based on this virtual server entry.
Server IP Address	This is the LAN IP address to which the ZyXEL Device forwards the incoming traffic.

7.3.1 Virtual Server Rule Add

To create a virtual server rule, click **Advanced Setup** > **NAT** > **Virtual Servers** > **Add** to open the following screen.

Figure 35 Advanced Setup > NAT > Virtual Servers > Add


NAT -- Virtual Servers
Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.
Remaining number of entries that can be configured:32
Server Name:
Select a Service:
Select One
Custom Server:
Server IP Address:
192.168.1.
Save/Apply
External Port Start
External Port End
Protocol
Internal Port Start
Internal Port End
TCP
Save/Apply

The following table describes the fields in this screen.

Table 21 Advanced Setup > NAT > Virtual Servers > Add

LABEL	DESCRIPTION
Server Name	Either select a pre-defined service or select **Custom Server** and enter a name manually.
Server IP Address	Enter the LAN IP address to which the ZyXEL Device should forward the traffic.
Save/Apply	When using a pre-defined service, if you do not want to modify the port numbers, you can click this button to save the changes and have the ZyXEL Device start using them.
External Port Start	Enter a port number in this field. To forward only one port, enter the port number again in the **External Port End** field. To forward a series of ports, enter the start port number here and the end port number in the **External Port End** field.
External Port End	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Protocol	This is the underlying protocol of the traffic to which this virtual server entry applies.

Table 21 Advanced Setup > NAT > Virtual Servers > Add (continued)

LABEL	DESCRIPTION
Internal Port Start	Specify the starting port the ZyXEL Device uses for the traffic that it forwards based on this virtual server entry (or leave it the same as the External
Internal Port End	The ZyXEL Device automatically determines this port number.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

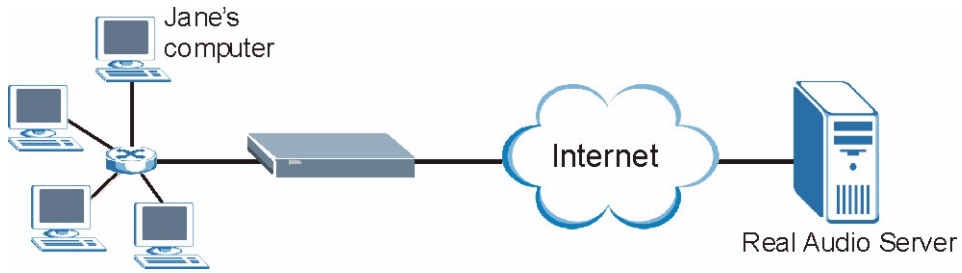
7.4 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyXEL Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyXEL Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 36 Trigger Port Forwarding Process: Example

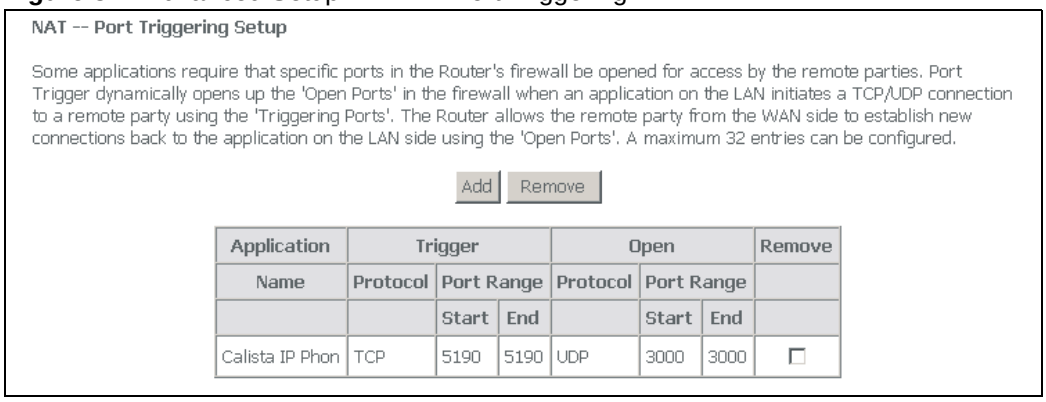


1. Jane (A) requests a file from the Real Audio server (port 7070).
2. Port 7070 is a “trigger” port and causes the ZyXEL Device to record Jane’s computer IP address. The ZyXEL Device associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The ZyXEL Device forwards the traffic to Jane’s computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyXEL Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Advanced Setup > NAT** > **Port Triggering** to open the following screen. Use this screen to change your ZyXEL Device's trigger port settings.

Figure 37 Advanced Setup > NAT > Port Triggering


NAT -- Port Triggering Setup
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.
Add
Remove
Application
Trigger
Open
Remove
Name
Protocol
Port Range
Protocol
Port Range
Start
End
Start
End
Calista IP Phon
TCP
5190
5190
UDP
3000
3000

The following table describes the labels in this screen.

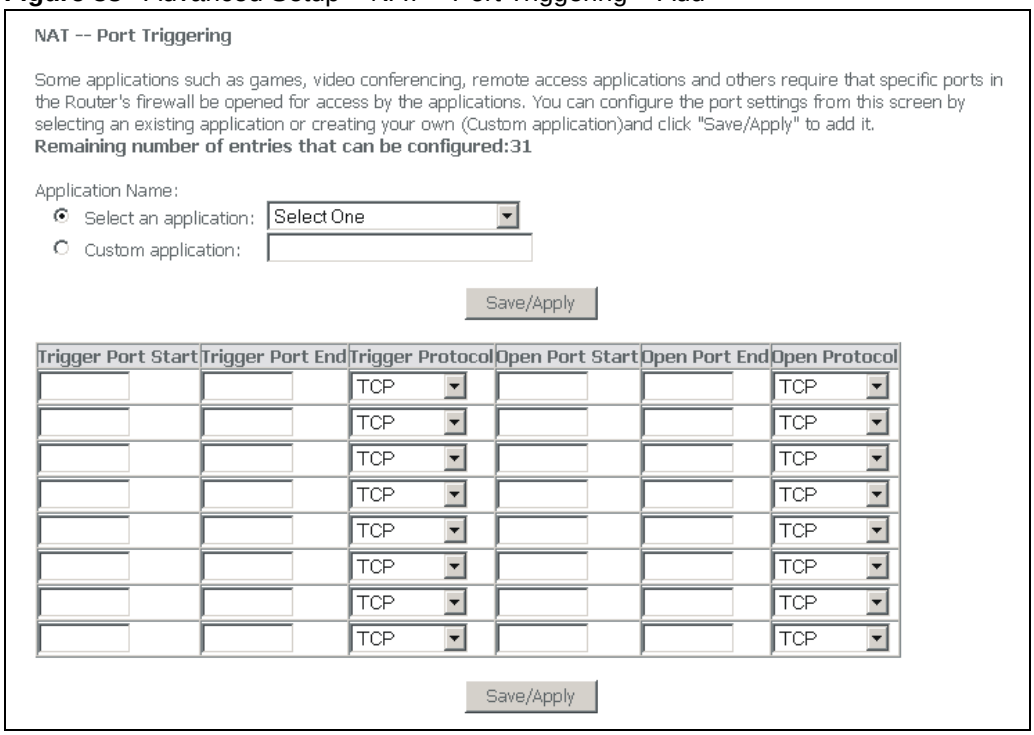
Table 22 Advanced Setup > NAT > Port Triggering

LABEL	DESCRIPTION
Add	Click this button to go to a screen where you can configure a new entry.
Remove	To remove an entry(ies), select its **Remove** check box and click the **Remove** button.
Application	Name for identification purposes.
Trigger	The trigger port is a protocol and port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Open	Open is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.

7.5 Port Triggering Add

Click **Advanced Setup > NAT** > **Port Triggering > Add** to open the following screen. Use this screen to change your ZyXEL Device's trigger port settings.

Figure 38 Advanced Setup > NAT > Port Triggering > Add


NAT -- Port Triggering
Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.
Remaining number of entries that can be configured:31
Application Name:
Select an application:
Select One
Custom application:
Save/Apply
Trigger Port Start
Trigger Port End
Trigger Protocol
Open Port Start
Open Port End
Open Protocol
TCP
Save/Apply

The following table describes the labels in this screen.

Table 23 Advanced Setup > NAT > Port Triggering > Add

LABEL	DESCRIPTION
Application Name	Either select a pre-defined application or select **Custom Application** and enter a name manually.
Save/Apply	When using a pre-defined service, if you do not want to modify the port numbers, you can click this button to save the changes and have the ZyXEL Device start using them.
Trigger	The trigger port is a protocol and port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Trigger Port Start	Type a port number or the starting port number in a range of port numbers.
Trigger Port End	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the protocol.
Open	Open is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Open Start Port	Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the protocol.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

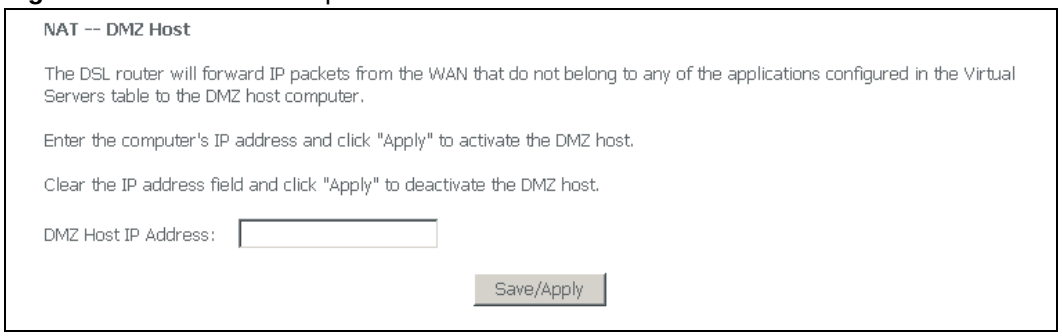
7.6 DMZ Host

In addition to the virtual servers for specified services, NAT supports a DMZ host IP address. The DMZ host receives packets from ports that are not specified in the applications in the virtual server configuration.

If you do not assign a DMZ host IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Click **Advanced Setup** > **NAT** > **DMZ Host** to open the following screen. Use this screen to specify a DMZ host IP address.

Figure 39 Advanced Setup > NAT > DMZ Host


NAT -- DMZ Host
The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.
DMZ Host IP Address:
Save/Apply

The following table describes the labels in this screen.

Table 24 Advanced Setup > NAT > Port Triggering > Add

LABEL	DESCRIPTION
DMZ Host IP Address	Specify the IP address of the LAN computer to which you want to send packets from ports that are not specified in the applications in the virtual server configuration.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

8

Security

This chapter describes how to configure security settings.

8.1 Outgoing IP Filtering

By default, the ZyXEL Device allows traffic from the LAN to go to the Internet. Click **Advanced Setup** > **Security** > **IP Filtering** > **Outgoing** to open the following screen. This screen lists the currently configured filtering entries.

Figure 40 Advanced Setup > Security > IP Filtering > Outgoing

The following table describes the labels in this menu.

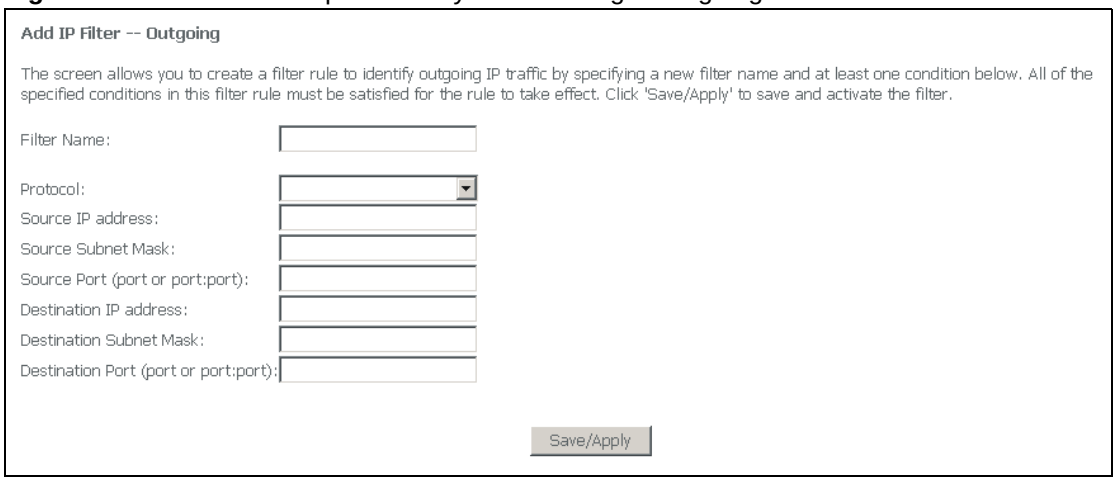
Table 25 Advanced Setup > Security > IP Filtering > Outgoing

LABEL	DESCRIPTION
Filter Name	This is the name configured to identify the filter entry.
Protocol	This is the type of packets to which this entry applies.
Source Address / Mask	This is the IP address and subnet mask of a LAN computer to which this entry applies.
Source Port	This is the source port for traffic (from the LAN) to which this entry applies.
Dest. Address / Mask	This is the IP address and subnet mask of a computer on the Internet to which this entry applies.
Dest. Port	This is the destination port for traffic to which this entry applies.
Remove	To remove a rule, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new entry.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.

8.2 Adding Outgoing IP Filtering Rules

To add an outgoing IP filtering rule, click **Advanced Setup** > **Security** > **IP Filtering** > **Outgoing** > **Add**. The screen appears as shown.

Figure 41 Advanced Setup > Security > IP Filtering > Outgoing > Add


Add IP Filter -- Outgoing
The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.
Filter Name:
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
Save/Apply

The following table describes the labels in this menu.

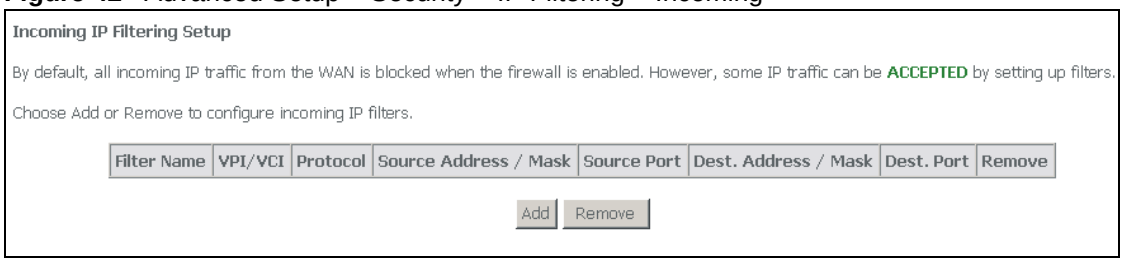
Table 26 Advanced Setup > Security > IP Filtering > Outgoing > Add

LABEL	DESCRIPTION
Filter Name	Type the name configured to identify the filter entry.
Protocol	Select the type of packets to which this entry applies (TCP, UDP, or both).
Source IP Address	Type the IP address of a LAN computer to which this entry applies.
Source Subnet Mask	Type the subnet mask of a LAN computer to which this entry applies.
Source Port	Type the source port for traffic (from the LAN) to which this entry applies.
Destination IP Address	This is the IP address and subnet mask of a computer on the Internet to which this entry applies.
Destination Subnet Mask	Type the subnet mask of a computer on the Internet to which this entry applies.
Destination Port	Type the destination port for traffic to which this entry applies.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

8.3 Incoming IP Filtering

By default, the ZyXEL Device blocks traffic from the Internet from going to the LAN. Use incoming IP filtering to allow certain traffic to come in from the Internet to the LAN. For example, you could allow access to a web server on your LAN to let people access a website that it is hosting. Click **Advanced Setup** > **Security** > **IP Filtering** > **Incoming** to open the following screen. This screen lists the currently configured filtering entries.

Figure 42 Advanced Setup > Security > IP Filtering > Incoming


Incoming IP Filtering Setup
By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be ACCEPTED by setting up filters.
Choose Add or Remove to configure incoming IP filters.
Filter Name
VPI/VCI
Protocol
Source Address / Mask
Source Port
Dest. Address / Mask
Dest. Port
Remove
Add
Remove

The following table describes the labels in this menu.

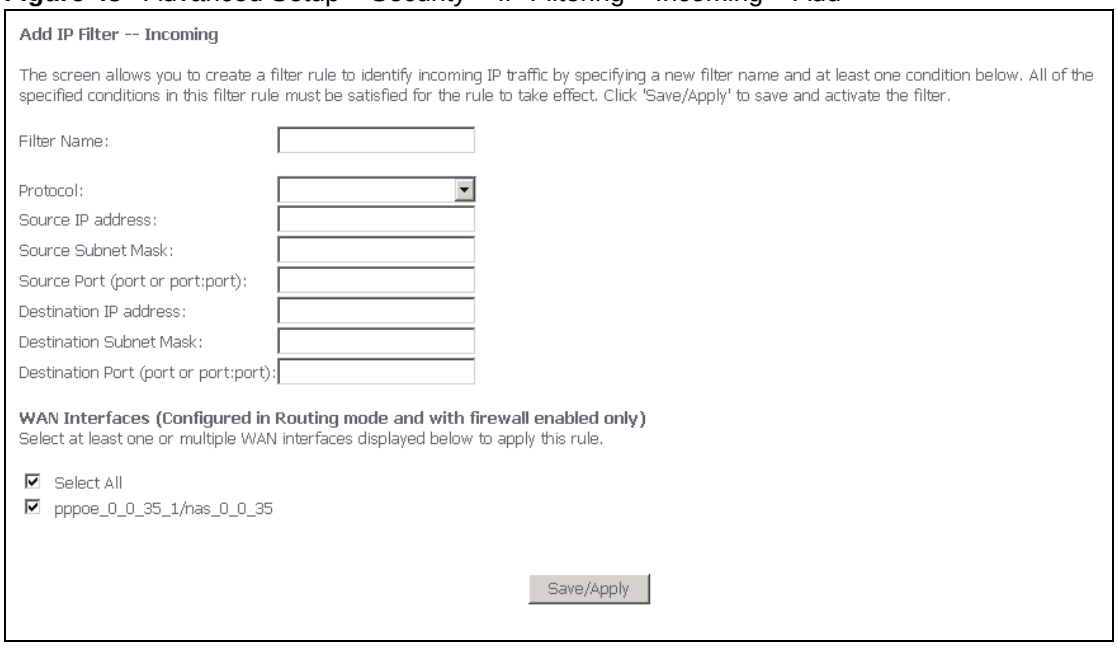
Table 27 Advanced Setup > Security > IP Filtering > Incoming

LABEL	DESCRIPTION
Filter Name	This is the name configured to identify the filter entry.
VPI/VCI	This is the WAN connection's Virtual Path Identifier, and Virtual Channel Identifier.
Protocol	This is the type of packets to which this entry applies.
Source Address / Mask	This is the IP address and subnet mask of a computer (on the Internet) to which this entry applies.
Source Port	This is the source port for traffic (from the Internet) to which this entry applies.
Dest. Address / Mask	This is the IP address and subnet mask of a LAN computer to which this entry allows traffic from the Internet.
Dest. Port	This is the destination port for traffic to which this entry applies.
Remove	To remove a rule, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new entry.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.

8.4 Adding Incoming IP Filtering Rules

To add an incoming IP filtering rule, click **Advanced Setup** > **Security** > **IP Filtering** > **Incoming** > **Add**. The screen appears as shown.

Figure 43 Advanced Setup > Security > IP Filtering > Incoming > Add


Add IP Filter -- Incoming
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.
Filter Name:
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.
Select All
pppoe_0_0_35_1/nas_0_0_35
Save/Apply

The following table describes the labels in this menu.

Table 28 Advanced Setup > Security > IP Filtering > Incoming > Add

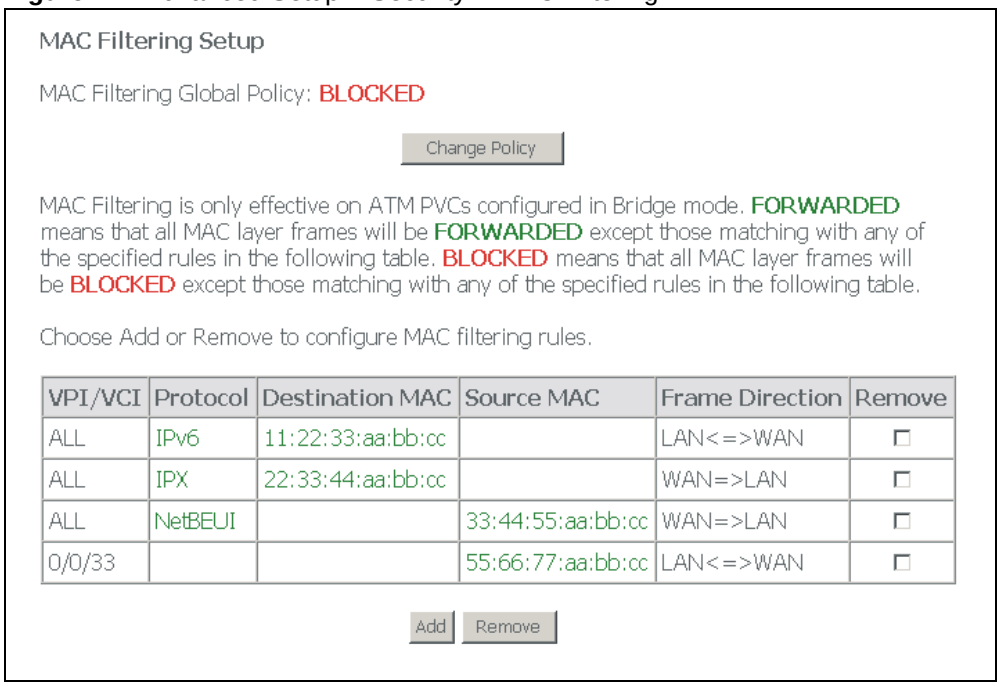
LABEL	DESCRIPTION
Filter Name	Type the name configured to identify the filter entry.
Protocol	Select the type of packets to which this entry applies (TCP, UDP, or both).
Source IP Address	Type the IP address of a computer on the Internet to which this entry applies.
Source Subnet Mask	Type the subnet mask of a computer on the Internet to which this entry applies.
Source Port	Type the source port for traffic (from the Internet) to which this entry applies.
Destination IP Address	This is the IP address and subnet mask of a LAN computer to which this entry allows access.
Destination Subnet Mask	Type the subnet mask of the LAN computer to which this entry applies.
Destination Port	Type the destination port for traffic to which this entry applies.
WAN Interfaces	Select the WAN interface(s) to which this rule applies.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

8.5 MAC Filtering

Configure the MAC filter to block or allow access based on MAC addresses. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your ZyXEL Device's MAC filter settings, click **Advanced Setup** > **Security** > **MAC Filtering**. The screen appears as shown. You need to know the MAC addresses of the devices to configure this screen.

Figure 44 Advanced Setup > Security > MAC Filtering



The following table describes the labels in this menu.

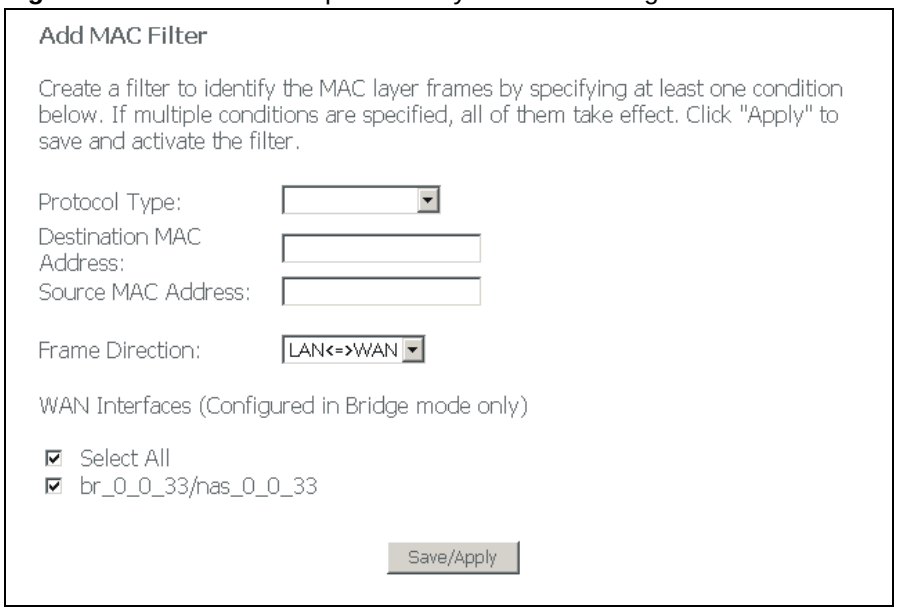
Table 29 Advanced Setup > Security > MAC Filtering

LABEL	DESCRIPTION
MAC Filtering Global Policy	**FORWARDED** has the ZyXEL Device forward traffic for all MAC addresses except the ones in the MAC filtering rules table below. **BLOCKED** has the ZyXEL Device block traffic for all MAC addresses except the ones in the MAC filtering rules table below. Click **Change Policy** to reverse this setting.
VPN/VCI	The port (interface), VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) identify the ATM PVC (Permanent Virtual Circuit) to which this rule applies.
Protocol	This is the type of packets to which this rule applies. Blank means all types.
Destination MAC	The destination MAC addresses (in XX:XX:XX:XX:XX:XX format) of traffic that is allowed or not allowed to go through the ZyXEL Device. Blank means all destination MAC addresses.
Source MAC	The source MAC addresses (in XX:XX:XX:XX:XX:XX format) of traffic that is allowed or not allowed to go through the ZyXEL Device. Blank means all source MAC addresses.
Frame Direction	This is the direction of packet flow to which the rule applies.
Remove	To remove a rule, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new MAC filtering rule.
Remove	To remove a WAN connection, select its **Remove** check box and click the **Remove** button.

8.6 MAC Filtering Rules

To add a MAC filtering rule, click **Advanced Setup** > **Security** > **MAC Filtering** > **Add**. The screen appears as shown.

Figure 45 Advanced Setup > Security > MAC Filtering > Add


Add MAC Filter
Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.
Protocol Type:
Destination MAC Address:
Source MAC Address:
Frame Direction:
LAN<=>WAN
WAN Interfaces (Configured in Bridge mode only)
Select All
br_0_0_33/nas_0_0_33
Save/Apply

The following table describes the labels in this menu.

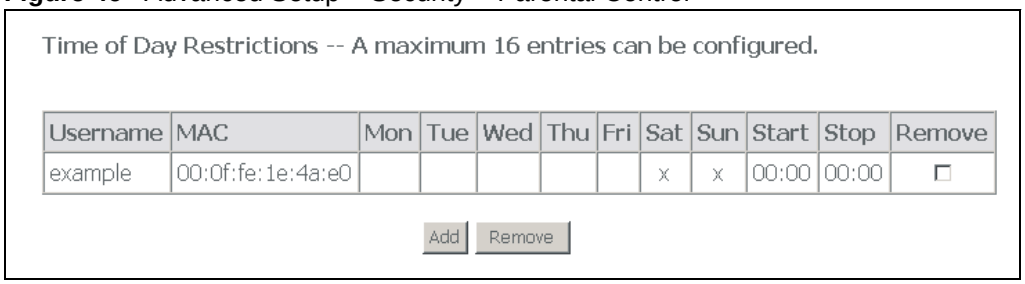
Table 30 Advanced Setup > Security > MAC Filtering > Add

LABEL	DESCRIPTION
Protocol	Select the type of packets to which this rule applies. Leave it blank to apply the rule to all types of packets.
Destination MAC	Enter the destination MAC address (in XX:XX:XX:XX:XX:XX format) of traffic that is allowed or not allowed to go through the ZyXEL Device. Leave it blank to apply the rule to traffic going to any MAC address.
Source MAC	Enter the source MAC addresses (in XX:XX:XX:XX:XX:XX format) of traffic that is allowed or not allowed to go through the ZyXEL Device. Leave it blank to apply the rule to traffic coming from any MAC address.
Frame Direction	Select the direction of packet flow to which the rule applies.
WAN Interfaces	Select the WAN interface(s) to which this rule applies.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

8.7 Parental Control (Blocking Schedule)

Click **Advanced Setup** > **Security** > **Parental Control** to display the following screen. This screen shows policies controlling which days and times Internet access is blocked from specific MAC addresses.

Figure 46 Advanced Setup > Security > Parental Control



The following table describes the labels in this screen.

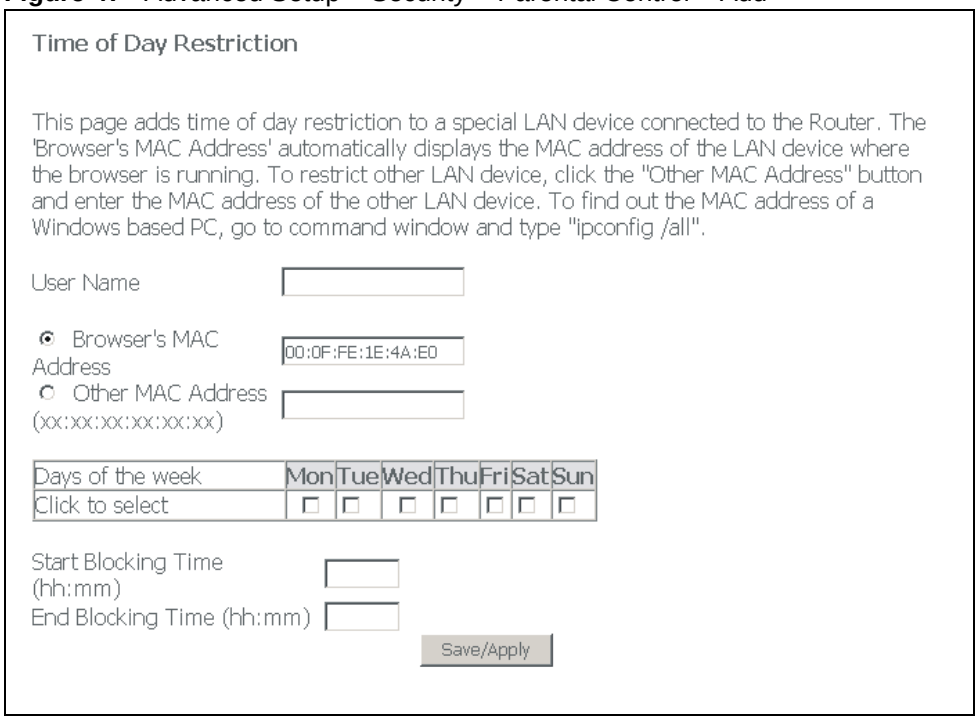
Table 31 Advanced Setup > Security > Parental Control

LABEL	DESCRIPTION
Username	This name identifies to whom the blocking schedule applies.
MAC	This is the MAC address of the computer to which this blocking schedule applies.
Mon ~ Sun	These fields show to which days of the week the blocking schedule applies.
Start	This is the beginning time for the blocked access period.
Stop	This is the ending time for the blocked access period.
Add	Click this button to go to a screen where you can configure settings for a new entry.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.

8.8 Adding Parental Control (Blocking Schedule) Entries

Click **Advanced Setup** > **Security** > **Parental Control** > **Add** to display the following screen. Use this screen to configure which days and times Internet access is blocked from a specific MAC address.

Figure 47 Advanced Setup > Security > Parental Control > Add


Time of Day Restriction
This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".
User Name
Browser's MAC Address
00:0F:FE:1E:4A:E0
Other MAC Address (xx:xx:xx:xx:xx:xx)
Days of the week
Mon Tue Wed Thu Fri Sat Sun
Click to select
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Save/Apply

The following table describes the labels in this screen.

Table 32 Advanced Setup > Security > Parental Control > Add

LABEL	DESCRIPTION
Username	Enter a name to identify to whom the blocking schedule applies.
Browser's MAC	Select this to use the MAC address of the computer you are currently using to manage the ZyXEL Device.
Other MAC Address	Select this to manually enter the MAC address of a computer.
Days of the week	Select to which days of the week the blocking schedule applies.
Start Blocking Time	This is the beginning time for the blocking period. Include a two-digit number of hours followed by a colon and a. two-digit number of hours.
End Blocking Time	This is the ending time for the blocking period. Include a two-digit number of hours followed by a colon and a. two-digit number of hours.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

9

Quality of Service (QoS)

This chapter contains information about configuring QoS, editing classifiers and viewing the ZyXEL Device's QoS packet statistics.

9.1 QoS Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the ZyXEL Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1. Configure classifiers to sort traffic into different flows.
2. Assign priority and define actions to be performed for a classified traffic flow.

The ZyXEL Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

The ZyXEL Device applies QoS to upstream traffic (going out through the WAN interface).

9.1.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 33 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

9.1.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

9.1.3 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a Class of Service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

9.1.3.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

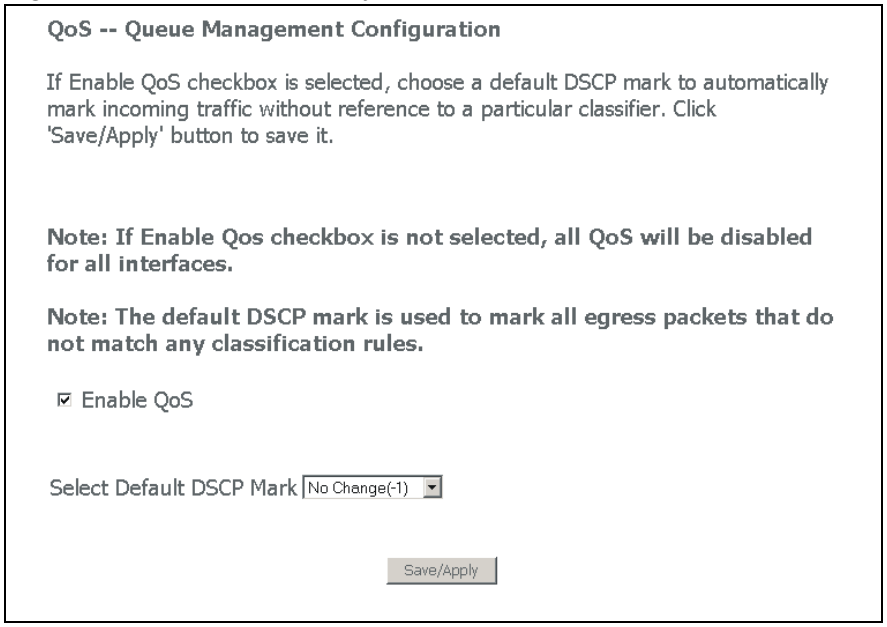
The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

9.2 Configuring QoS General Screen

Click **Advanced** > **Quality of Service** to open the screen as shown next.

Use this screen to enable or disable QoS, and select a DSCP mark to use on all outgoing packets that do not match a QoS classification rule.

Figure 48 Advanced > Quality of Service


QoS -- Queue Management Configuration
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Enable QoS
Select Default DSCP Mark
No Change(-1)
Save/Apply

The following table describes the labels in this screen.

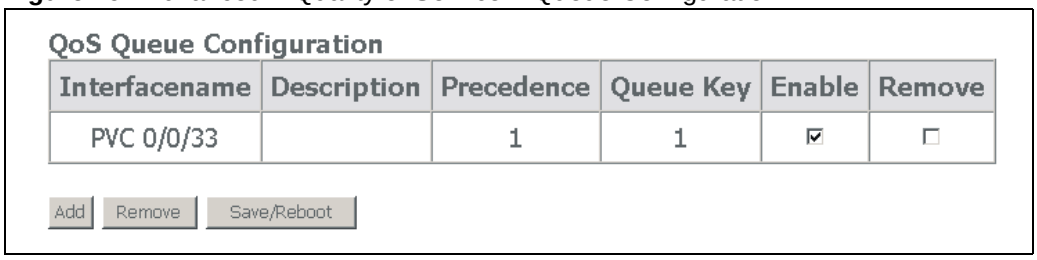
Table 34 Advanced > Quality of Service

LABEL	DESCRIPTION
Enable QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
Select Default DSCP Mark	Select a DSCP mark to use on all outgoing packets that do not match a QoS classification rule. You can select a specific DSCP mark to use or have the ZyXEL Device automatically select a DSCP mark to use.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

9.3 Queue Configuration

Click **Advanced** > **Quality of Service** > **Queue Configuration** to open the following screen. This screen lists the QoS queues. A QoS queue sets the priority used for incoming packets that the QoS classifier has grouped into a flow.

Figure 49 Advanced > Quality of Service > Queue Configuration



The following table describes the labels in this screen.

Table 35 Advanced > Quality of Service > Queue Configuration

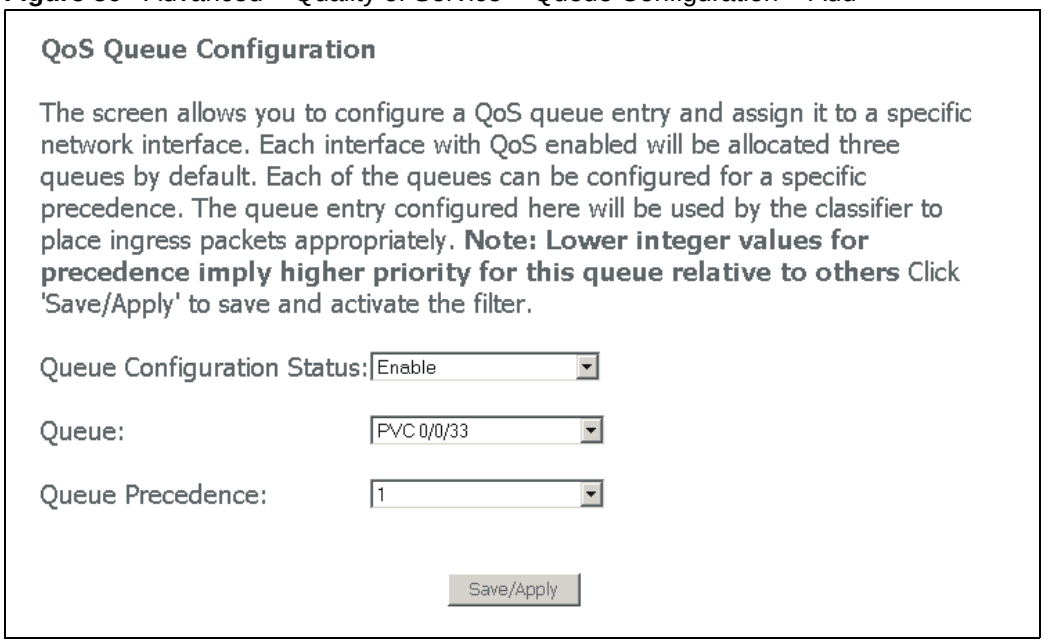
LABEL	DESCRIPTION
Interface name	This field displays the WAN connection's DSL port, Virtual Path Identifier, and Virtual Channel Identifier.
Description	This field displays any extra configured identification information.
Precedence	This shows the queue's priority relative to the other queues. The lower the number, the higher the priority. 1 is the highest priority. 4 is the lowest.
Queue Key	This is the queue entry's index number.
Enable	Select the check box to enable this classifier.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new QoS queue.
Remove	To remove an entry select its **Remove** check box and click the **Remove** button.
Save/Reboot	Click this button to apply and save your changes. The ZyXEL Device restarts.

9.4 Adding a Queue

Click **Advanced** > **Quality of Service** > **Queue Configuration** > **Add** to open the following screen. Use this screen to configure a QoS queue. A QoS queue sets the priority used for incoming packets that the QoS classifier has grouped into a flow.

You can only add QoS queues for WAN interfaces that have QoS enabled.

Figure 50 Advanced > Quality of Service > Queue Configuration > Add


QoS Queue Configuration
The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. Note: Lower integer values for precedence imply higher priority for this queue relative to others Click 'Save/Apply' to save and activate the filter.
Queue Configuration Status:
Enable
Queue:
PVC 0/0/33
Queue Precedence:
1
Save/Apply

The following table describes the labels in this screen.

Table 36 Advanced > Quality of Service > Queue Configuration > Add

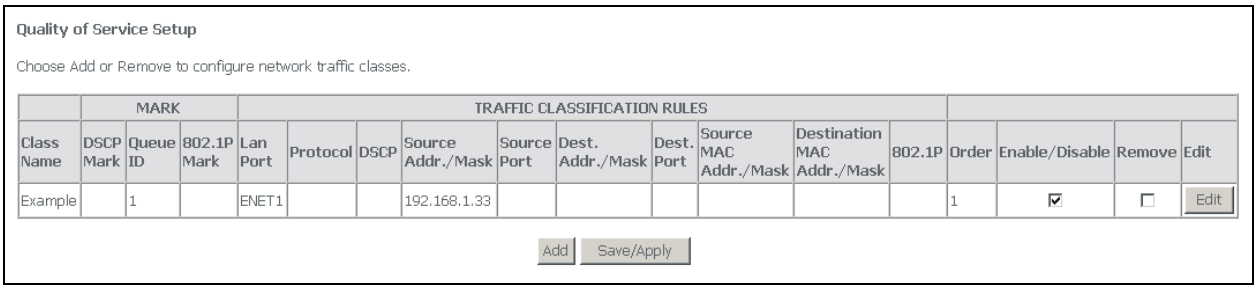
LABEL	DESCRIPTION
Queue Configuration Status	Select **Enable** to turn on this queue.
Queue	Select the WAN connection's DSL port, Virtual Path Identifier, and Virtual Channel Identifier.
Description	This field displays any extra configured identification information.
Queue Precedence	Set the queue's priority relative to the other queues. The lower the number, the higher the priority. 1 is the highest priority. 4 is the lowest.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

9.5 Class Setup

Click **Advanced** > **Quality of Service** > **QoS Classification** to open the following screen.

This screen lists the QoS classifiers. A classifier groups upstream traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow. The classifier also assigns a specific QoS queue, DSCP mark, and/or IEEE 802.1p tag.

Figure 51 Advanced > Quality of Service > QoS Classification



The following table describes the labels in this screen.

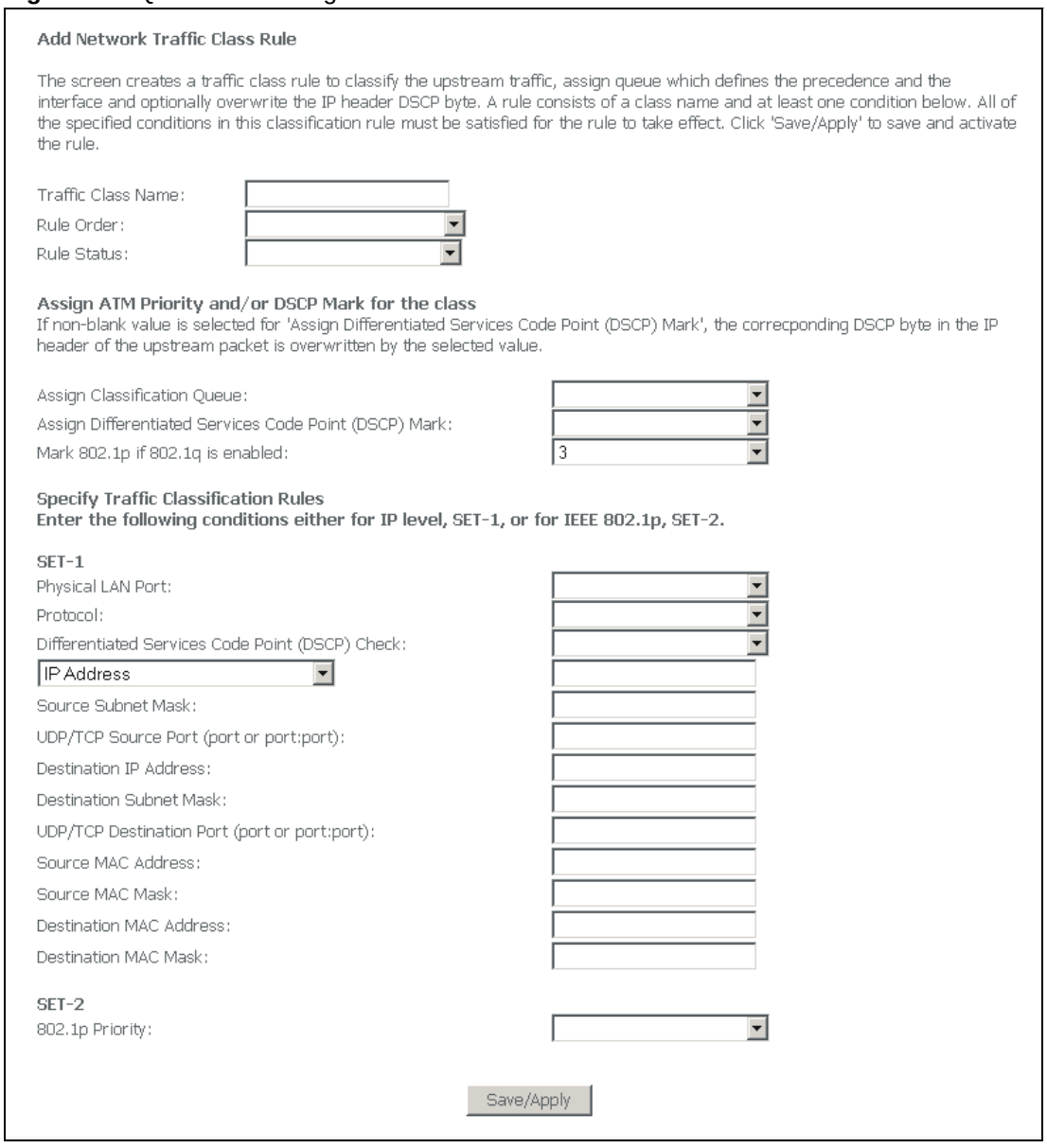
Table 37 Advanced > Quality of Service > QoS Classification

LABEL	DESCRIPTION
Class Name	This is the name of the classifier.
MARK	These columns are the QoS setting the ZyXEL Device uses for or assigns to the packets of upstream traffic that match this QoS classifier.
DSCP Mark	This is the DSCP mark the ZyXEL Device assigns to the packets of upstream traffic that match this QoS classifier.
Queue ID	This is the QoS queue the ZyXEL Device uses for the packets of upstream traffic that match this QoS classifier.
802.1P Mark	This is the IEEE 802.1p mark the ZyXEL Device assigns to the packets of upstream traffic that match this QoS classifier.
TRAFFIC CLASSIFICATION RULES	These columns identify the upstream traffic to which the QoS classifier applies.
Lan Port	This is the source Ethernet port of the traffic.
Protocol	This is the type of packets.
DSCP	This is the DSCP mark.
Source Addr./Mask	This is the IP address (and optionally the subnet mask) of the device that sent the traffic.
Source Port	This is the port number that a device used to send the traffic.
Dest. Addr./Mask	This is the IP address (and optionally the subnet mask) of the device that the traffic is going to.
Dest. Port	This is the port number on a device to which the traffic is going.
Source MAC Addr./ Mask	This is the MAC address (and optionally the subnet mask) of the device that sent the traffic.
Dest. MAC Addr./ Mask	This is the MAC address (and optionally the subnet mask) of the device that the traffic is going to.
802.1P	This is the IEEE 802.1p mark on the traffic.
Order	This is the classifier's place in the classifiers list.
Enable / Disable	The classifier is active when this check box is selected.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new QoS queue.
Remove	To remove an entry select its **Remove** check box and click the **Remove** button.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

9.5.1 Configuring a QoS Class

Click **Advanced** > **Quality of Service** > **QoS Classification** and then the **Add** or **Edit** button to configure a classifier. There are two sets of classification rules. Set-1 is based on different fields within the TCP/UDP/IP layer plus the physical LAN port. Set-2 is based on the MAC layer IEEE 802.1p priority field. Use one set or the other for a class (not both sets).

Figure 52 QoS Class Configuration


Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
Rule Order:
Rule Status:
Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.
Assign Classification Queue:
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:
3
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port:
Protocol:
Differentiated Services Code Point (DSCP) Check:
IP Address
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
SET-2
802.1p Priority:
Save/Apply

See Appendix D on page 185 for a list of commonly-used services. The following table describes the labels in this screen.

Table 38 QoS Class Configuration

LABEL	DESCRIPTION
Traffic Class Name	Type a name for the classifier.
Rule Order	Select the classifier's place in the classifiers list.

Table 38 QoS Class Configuration (continued)

LABEL	DESCRIPTION
Rule Status	Select whether or not the classifier is to be active.
Assign Classification Queue	Select the QoS queue the ZyXEL Device uses for the packets of upstream traffic that match this QoS classifier.
Assign Differentiated Services Code Point (DSCP) Mark	Select the DSCP mark the ZyXEL Device assigns to the packets of upstream traffic that match this QoS classifier.
Mark 802.1p if 802.1q is enabled	Select the IEEE 802.1p mark the ZyXEL Device assigns to the packets of upstream traffic that match this QoS classifier. This only applies when IEEE 802.1q is enabled. You enable IEEE 802.1q by enabling VLAN multiplexing in the WAN screens (see Section 5.4 on page 54).
Physical LAN Port	Select the source Ethernet port of the traffic.
Protocol	Select the type of packets.
Differentiated Services Code Point (DSCP) Check	Select the DSCP mark to check upstream traffic for.
IP Address/ Vendor Class ID (DHCP Option 60)/ User class ID (DHCP option 77)	Select whether to check for a source IP address, vendor class ID, or user class ID. Then specify the source IP address, vendor class ID, or user class ID.
Source Subnet Mask	Specify the subnet mask of the device that sent the traffic.
UDP/TCP Source Port (port or port:port)	This is the port number that a device used to send the traffic.
Destination IP Address	Specify the IP address of the device that the traffic is going to.
Destination Subnet Mask	Specify the subnet mask of the device that the traffic is going to.
UDP/TCP Destination Port (port or port:port)	Specify the port number on a device to which the traffic is going.
Source MAC Address	Specify the MAC address of the device that sent the traffic.
Source MAC Mask	Specify the MAC address subnet mask of the device that sent the traffic.
Destination MAC Address	Specify the MAC address of the device that the traffic is going to.
Destination MAC Mask	Specify the MAC address subnet mask of the device that the traffic is going to.
802.1p Priority	Specify the IEEE 802.1p mark on the traffic.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

10

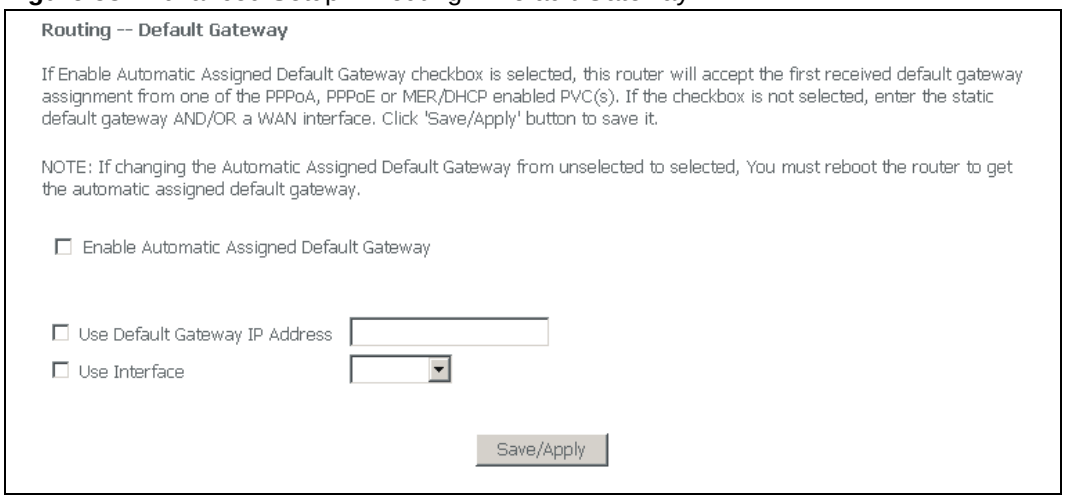
Routing

This chapter shows you how to configure the default gateway and static routes for your ZyXEL Device.

10.1 Default Gateway Setup

The default gateway is a neighboring router that helps the ZyXEL Device forward traffic to its destination. Click **Advanced** > **Routing** > **Default Gateway** to open the following screen. Use this screen to change the ZyXEL Device's default gateway settings.

Figure 53 Advanced Setup > Routing > Default Gateway


Routing -- Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Use Default Gateway IP Address
Use Interface
Save/Apply

The following table describes the labels in this screen.

Table 39 Advanced Setup > Routing > Default Gateway

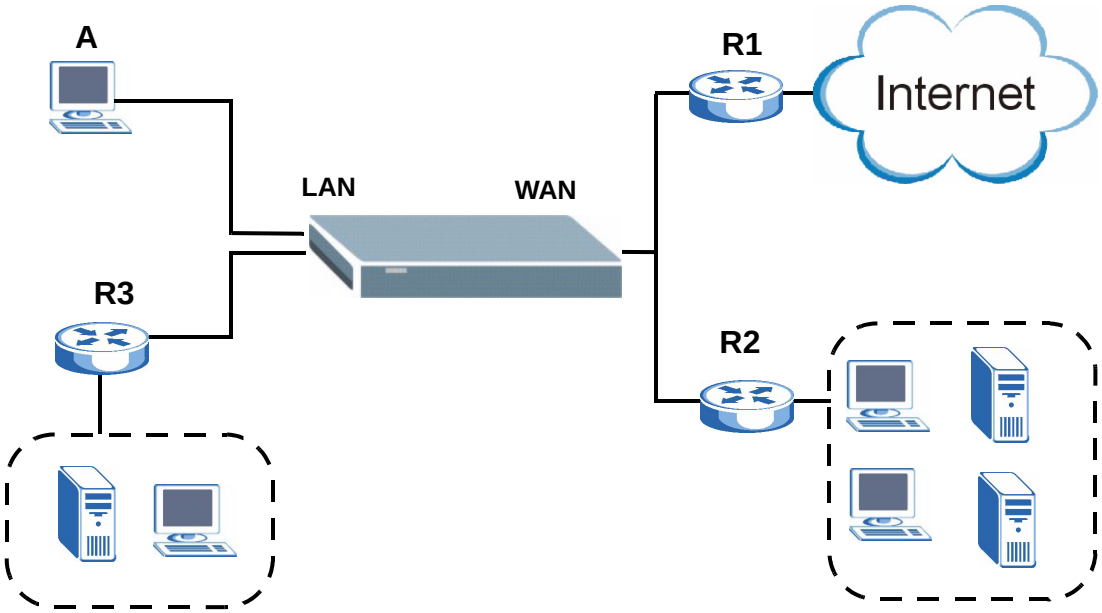
LABEL	DESCRIPTION
Enable Automatic Assigned Default Gateway	Select this option if the ISP did not give you the IP address of the default gateway. The ISP automatically assigns the WAN connection an IP address when it connects.
Use Default Gateway IP Address	If the ISP gave you a static (fixed) IP address, select this option and enter the connection's IP address.
Use Interface	To have the ZyXEL Device use a specific WAN interface for sending traffic to the default gateway, select this option and choose the WAN interface from the drop-down list box.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

10.2 Static Route

The ZyXEL Device usually uses the default gateway to route outbound traffic from local computers to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router (**R3**) connected to the LAN.

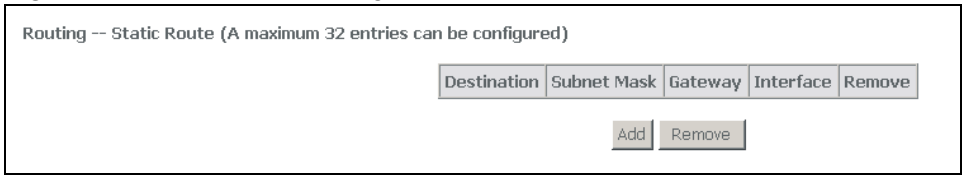
Figure 54 Example of Static Routing Topology



10.3 Configuring Static Route

Click **Advanced** > **Routing** > **Static Route** to open the **Static Route** screen.

Figure 55 Advanced > Routing > Static Route



The following table describes the labels in this screen.

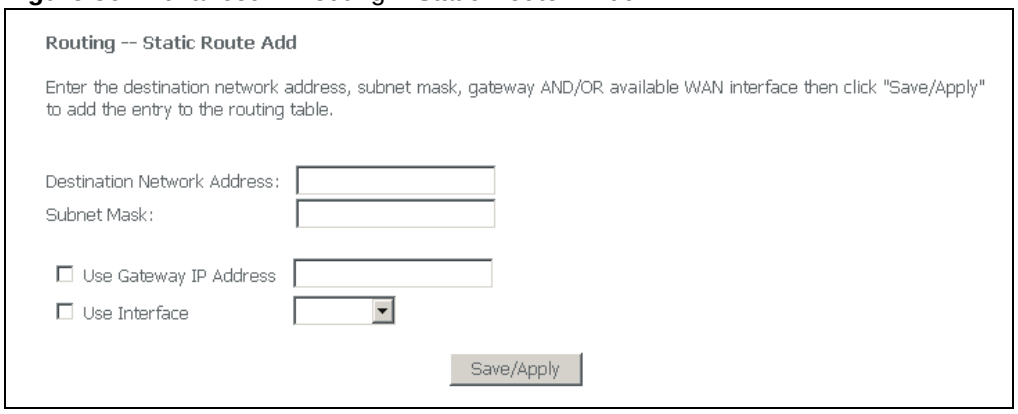
Table 40 Advanced > Routing > Static Route

LABEL	DESCRIPTION
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This is the IP subnet mask.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	If the static route should send traffic through a specific ZyXEL Device interface, it displays here.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new static route.
Remove	To remove an entry select its **Remove** check box and click the **Remove** button.

10.3.1 Static Route Add

Click **Advanced** > **Routing** > **Static Route** > **Add** to open the following screen. Use this screen to configure the required information for a static route.

Figure 56 Advanced > Routing > Static Route > Add


Routing -- Static Route Add
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.
Destination Network Address:
Subnet Mask:
Use Gateway IP Address
Use Interface
Save/Apply

The following table describes the labels in this screen.

Table 41 Advanced > Routing > Static Route > Add

LABEL	DESCRIPTION
Destination Network Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask of the destination network here.
Use Gateway IP Address	If you have a specific gateway IP address to enter, select this option and enter it in the field provided. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.

Table 41 Advanced > Routing > Static Route > Add

LABEL	DESCRIPTION
Interface	If the static route should send traffic through a specific ZyXEL Device interface, select this option and choose the interface.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

11

RIP

This chapter covers configuring the RIP settings for your ZyXEL Device.

11.1 RIP Setup

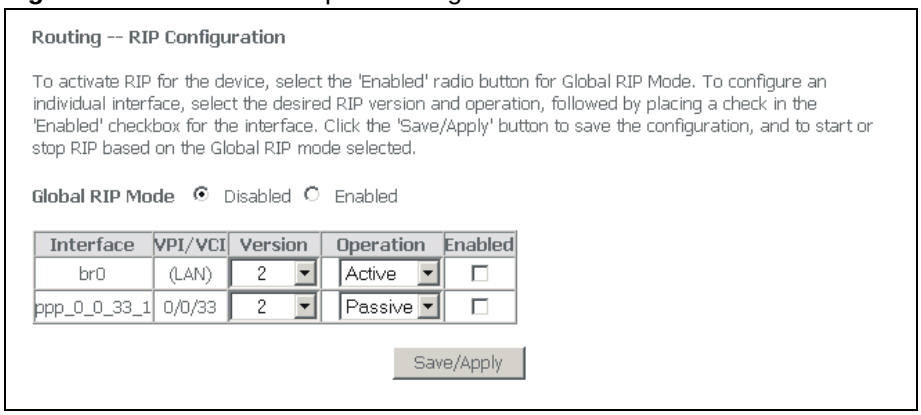
RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

Click **Advanced** > **Routing** > **RIP** to open the following screen. Use this screen to change the ZyXEL Device's RIP settings.

Figure 57 Advanced Setup > Routing > RIP


Routing -- RIP Configuration
To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.
Global RIP Mode
Disabled
Enabled
Interface
VPI/VCI
Version
Operation
Enabled
br0
(LAN)
2
Active
ppp_0_0_33_1
0/0/33
2
Passive
Save/Apply

The following table describes the labels in this screen.

Table 42 Advanced Setup > Routing > RIP

LABEL	DESCRIPTION
Global RIP Mode	Use these fields to turn RIP on or off for the whole ZyXEL Device. When you disable RIP, the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.
Interface	This field displays the name of the WAN connection.
VPN/VCI	The port (interface), VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) identify the ATM PVC (Permanent Virtual Circuit) to which these settings apply. “LAN” appears for a bridged connection.
Version	This field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.
Operation	RIP operation controls the sending and receiving of RIP packets. When set to **Active** the ZyXEL Device periodically broadcasts its routing table . When set to **Passive**, the ZyXEL Device uses the RIP information that it receives, but does not broadcast its routing table.
Enabled	Select or clear this field to turn RIP on or off for the interface.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

12

DNS Setup

This chapter describes how to configure DNS settings.

12.1 DNS Server Address

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them DNS server screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

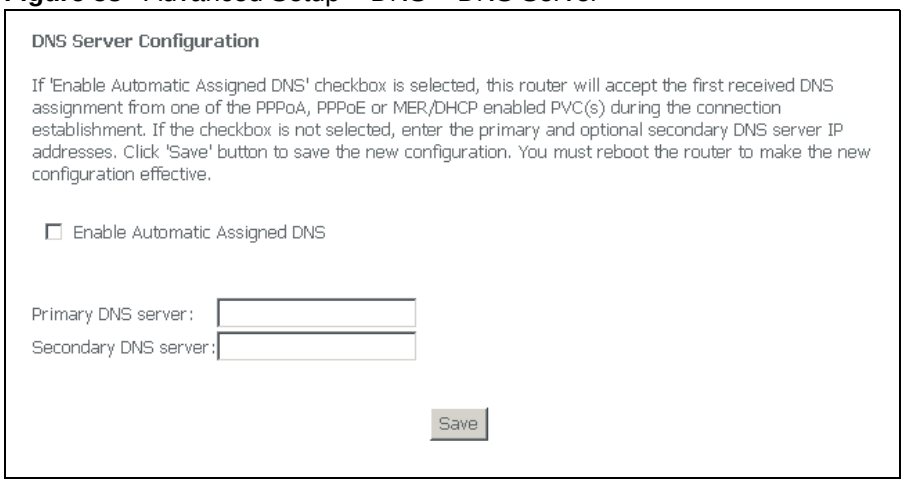
  The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left blank in the **LAN Setup** screen.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen.

12.2 DNS Setup

Click **Advanced Setup** > **DNS** > **DNS Server** to open the following screen.

Figure 58 Advanced Setup > DNS > DNS Server


DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.
Enable Automatic Assigned DNS
Primary DNS server:
Secondary DNS server:
Save

The following table describes the fields in this screen.

Table 43 Advanced Setup > DNS > DNS Server

LABEL	DESCRIPTION
Enable Automatic Assigned DNS	Select this option to have the ZyXEL Device accept and use the first DNS server IP address it gets from a WAN connection.
Primary DNS server Secondary DNS server	These fields are available when you clear **Enable Automatic Assigned DNS**. Enter the IP addresses of the DNS servers the ZyXEL Device is to use.
Save	Click **Save** to save your changes to the ZyXEL Device.

13

Dynamic DNS Setup

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

13.1 Dynamic DNS Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The dynamic DNS service provider will give you a password or key.

13.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

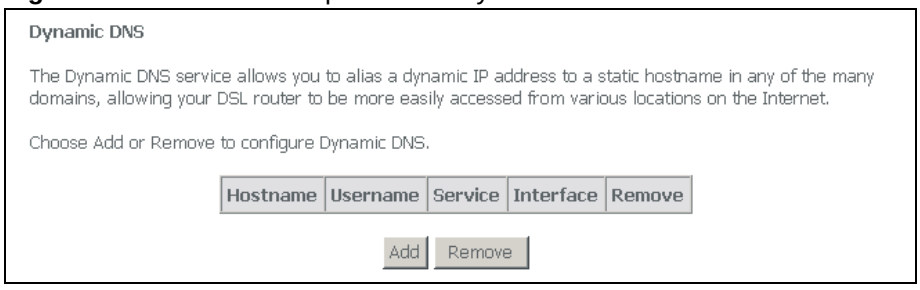
If you have a private WAN IP address, then you cannot use Dynamic DNS.

See Section 13.2 on page 105 for configuration instruction.

13.2 Dynamic DNS

Click **Advanced Setup** > **DNS** > **Dynamic DNS** to open the following screen.

Figure 59 Advanced Setup > DNS > Dynamic DNS


Dynamic DNS
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.
Choose Add or Remove to configure Dynamic DNS.
Hostname
Username
Service
Interface
Remove
Add
Remove

The following table describes the fields in this screen.

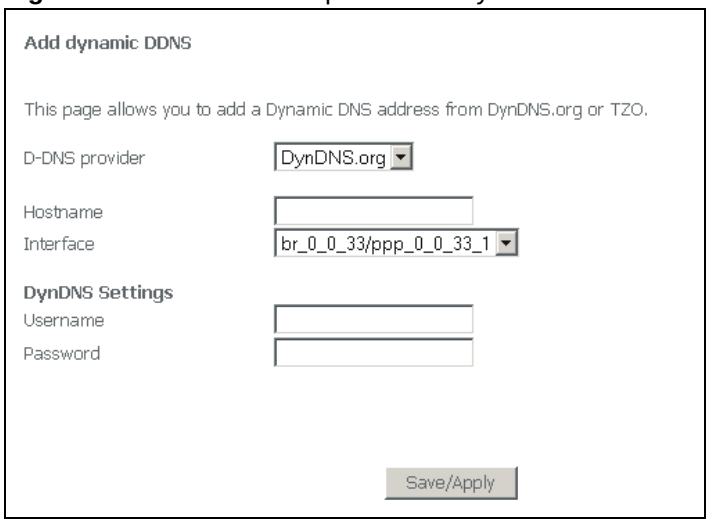
Table 44 Advanced Setup > DNS > Dynamic DNS

LABEL	DESCRIPTION
Host Name	This is the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.
User Name	This is the user name for the host name's DDNS account.
Service	This is the name of your Dynamic DNS service provider.
Interface	This is the ZyXEL Device's WAN connection that uses this DDNS host name.
Remove	To remove a DDNS entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new DDNS entry.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.

13.3 Configuring Dynamic DNS

Click **Advanced Setup** > **DNS** > **Dynamic DNS** > **Add** to open the following screen.

Figure 60 Advanced Setup > DNS > Dynamic DNS > Add



The following table describes the fields in this screen.

Table 45 Advanced Setup > DNS > Dynamic DNS > Add

LABEL	DESCRIPTION
D-DNS Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your dynamic DNS provider.
Interface	Select the ZyXEL Device's WAN connection that uses this DDNS host name.
Active Dynamic DNS	Select this check box to use dynamic DNS.
Username	Type your user name for this DDNS host name.

Table 45 Advanced Setup > DNS > Dynamic DNS > Add (continued)

LABEL	DESCRIPTION
Password	Type the password assigned for this DDNS host name.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

14

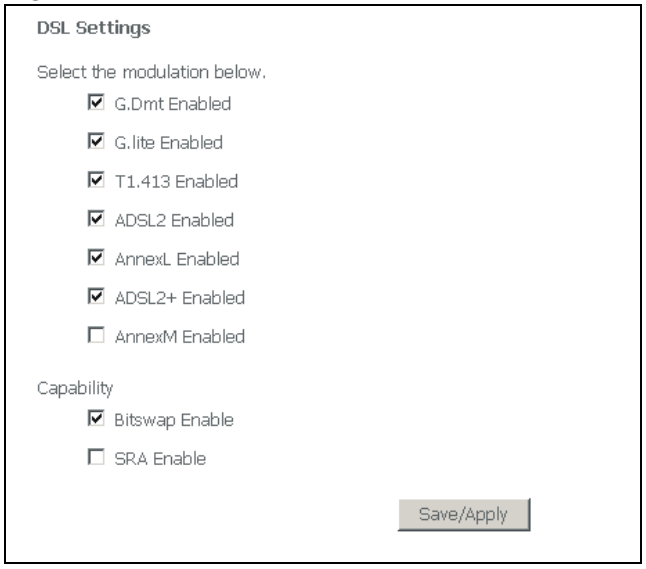
DSL Setup

This chapter explains how to configure ADSL port settings.

14.1 DSL Setup

Click **Advanced** > **DSL** to open the following screen where you can configure the ZyXEL Device's DSL settings.

Figure 61 Advanced > DSL



The following table describes the labels in this screen.

Table 46 Advanced > DSL

LABEL	DESCRIPTION
Select the modulation below	Select the port's ADSL operational mode. Select multiple modes to let the ZyXEL Device and the DSLAM automatically determine the mode to use. **AnnexL** (reach extended ADSL2) is an ADSL2+ mode that allows increased connection distances. **AnnexM** (double upstream mode) is an ADSL2+ mode that has the upstream connection use tones 6 to 63.
Bitswap Enable	Enable bit-swapping to allow the ZyXEL Device to adapt to line changes. It is recommended that you leave this enabled.

Table 46 Advanced > DSL (continued)

LABEL	DESCRIPTION
SRA Enable	Enable Seamless Rate Adaptation (SRA) to have the ZyXEL Device automatically adjust the connection's data rate according to line conditions without interrupting service.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

15

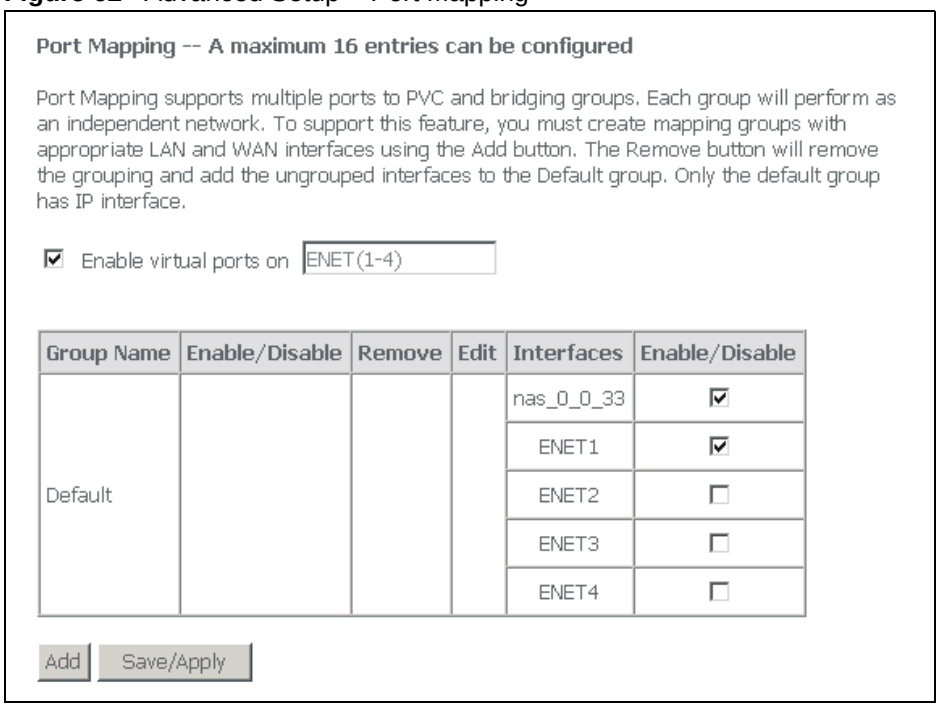
Port Mapping

This chapter explains how to map ports to PVCs and create bridging groups.

15.1 Port Mapping Setup

Click **Advanced Setup** > **Port Mapping** to open the following screen. Use this screen to map ports to PVCs and create bridging groups.

Figure 62 Advanced Setup > Port Mapping


Port Mapping -- A maximum 16 entries can be configured
Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.
Enable virtual ports on
ENET(1-4)
Group Name
Enable/Disable
Remove
Edit
Interfaces
Enable/Disable
Default
nas_0_0_33
ENET1
ENET2
ENET3
ENET4
Add
Save/Apply

The following table describes the labels in this screen.

Table 47 Advanced Setup > Port Mapping

LABEL	DESCRIPTION
Enable virtual ports on	Select this option to treat the LAN ports as separate (virtual) interfaces.
Group Name	This is the name configured to identify the group.
Enable/Disable	Use this column to turn the entire group on or off.
Remove	To remove an entry, select its **Remove** check box and click the **Save/Apply** button.

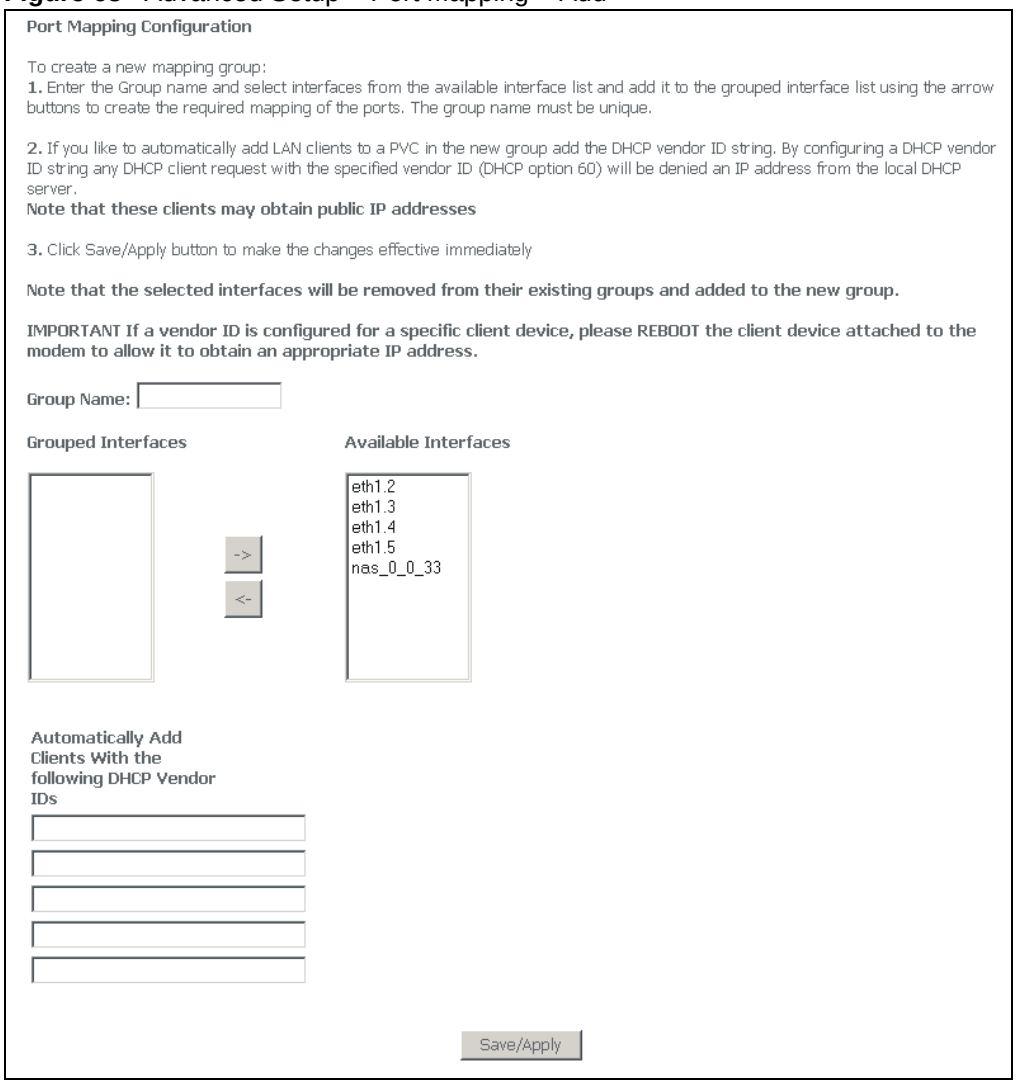
Table 47 Advanced Setup > Port Mapping (continued)

LABEL	DESCRIPTION
Edit	Click Edit to configure the group's settings.
Interfaces	These are the interfaces that belong to the group.
Enable/Disable	Use this column to turn an individual interface on or off.
Add	Click **Add** to open a screen where you can add a new entry.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

15.2 Adding a Port Mapping

Click **Advanced Setup** > **Port Mapping** > **Add** to open the following screen. Use this screen to map ports to PVCs and create bridging groups.

Figure 63 Advanced Setup > Port Mapping > Add


Port Mapping Configuration
To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses
3. Click Save/Apply button to make the changes effective immediately
Note that the selected interfaces will be removed from their existing groups and added to the new group.
IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
Group Name:
Grouped Interfaces
Available Interfaces
eth1.2
eth1.3
eth1.4
eth1.5
nas_0_0_33
->
<-
Automatically Add Clients With the following DHCP Vendor IDs
Save/Apply

The following table describes the labels in this screen.

Table 48 Advanced Setup > Port Mapping > Add

LABEL	DESCRIPTION
Group Name	Configure a name to identify the group.
Grouped Interfaces Available Interfaces	Select interfaces to add to the group.
Automatically Add Clients With the following DHCP Vendor IDs	If you want LAN clients to get public IP addresses, you can list their DHCP vendor IDs here.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

PART III
Diagnostics and Management

Diagnostics (117)
Settings (119)
Logs (123)
SNMP (127)
Time (131)
Access Control (133)
Update Software (137)
Save/Reboot and Logout (139)

16

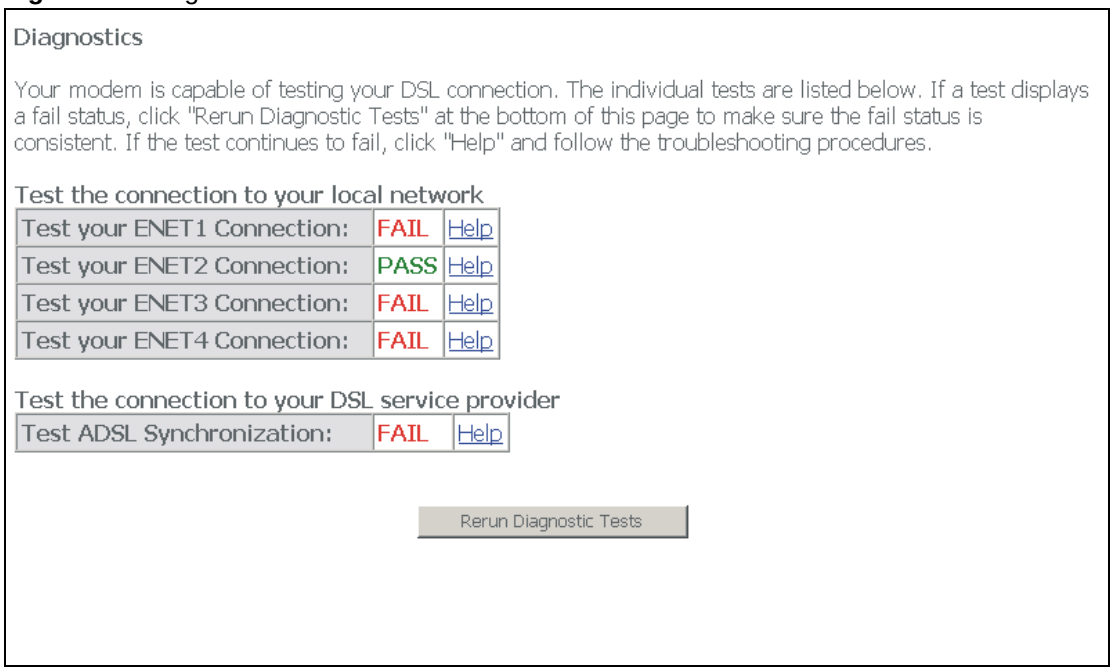
Diagnostics

These read-only screens display information to help you identify problems with the ZyXEL Device.

16.1 Diagnostics

Click **Diagnostics** to open the screen shown next. Use this screen to test the ZyXEL Devices connections. The ENET connections appear as four separate connections when you enable virtual ports (see Chapter 15 on page 111), otherwise they appear as a single connection. Both ADSL lines must be connected and working to pass the ADSL synchronization test.

Figure 64 Diagnostics


Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET1 Connection: FAIL Help
Test your ENET2 Connection: PASS Help
Test your ENET3 Connection: FAIL Help
Test your ENET4 Connection: FAIL Help
Test the connection to your DSL service provider
Test ADSL Synchronization: FAIL Help
Rerun Diagnostic Tests

17

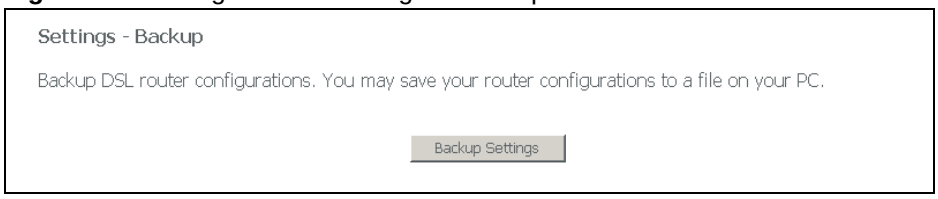
Settings

This chapter describes how to manage your ZyXEL Device's configuration.

17.1 Backup Configuration Using the Web Configurator

Click **Management** > **Settings** > **Backup** to open the following screen. Use this screen to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Figure 65 Management > Settings > Backup


Settings - Backup
Backup DSL router configurations. You may save your router configurations to a file on your PC.
Backup Settings

Click **Backup Settings** to save the ZyXEL Device's current configuration to your computer.

17.2 Restore Configuration Using the Web Configurator

Click **Management** > **Settings** > **Update** to open the following screen. Use this screen to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

Figure 66 Management > Settings > Update

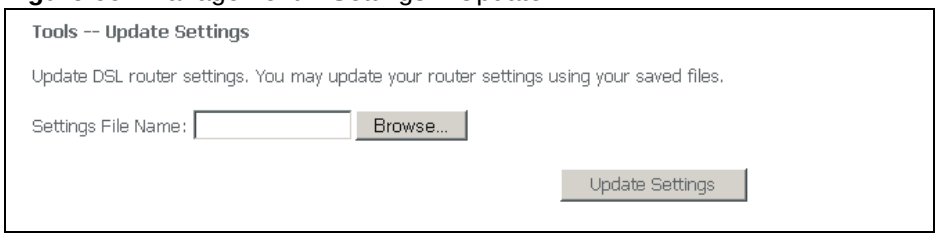

Tools -- Update Settings
Update DSL router settings. You may update your router settings using your saved files.
Settings File Name:
Browse...
Update Settings

Table 49 Management > Settings > Update

LABEL	DESCRIPTION
Settings File Name	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Update Settings	Click this to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress

You must then wait before logging into the ZyXEL Device again. The ZyXEL Device automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

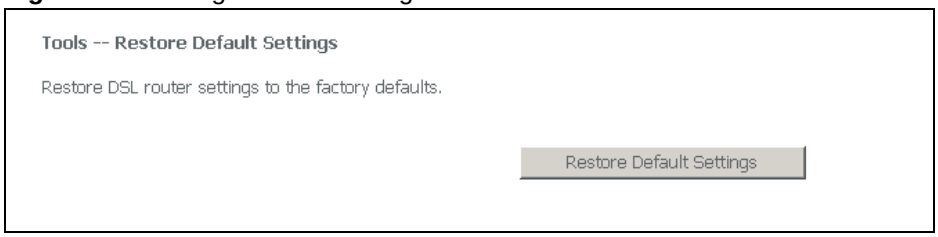
Figure 67 Temporarily Disconnected

You may need to change the IP address of your computer to be in the same subnet as that of the ZyXEL Device's IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

17.3 Restoring Factory Defaults

Click **Management** > **Settings** > **Restore Default** to open the following screen.

Figure 68 Management > Settings > Restore Default



Click **Restore Default Settings** to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device.

You may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

18

Logs

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs. Refer to the appendix for example log message explanations.

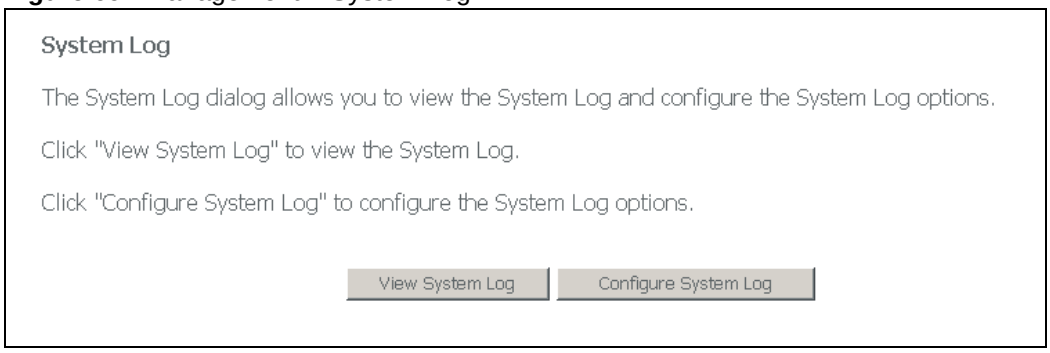
18.1 Logs Overview

The web configurator allows you to choose which levels of events to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

18.2 System Log

Click **Management** > **System Log** to open the following screen. Click **View System Log** screen to see the logs, or **Configure System Log** to configure the logging settings.

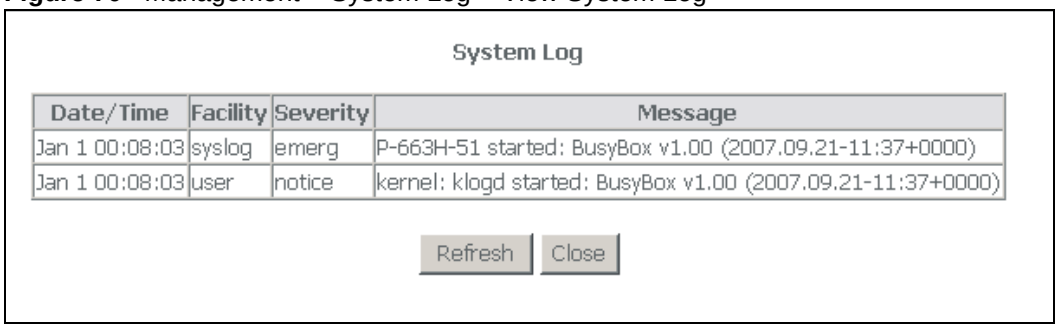
Figure 69 Management > System Log


System Log
The System Log dialog allows you to view the System Log and configure the System Log options.
Click "View System Log" to view the System Log.
Click "Configure System Log" to configure the System Log options.
View System Log
Configure System Log

18.3 Viewing the System Log

Click **Management** > **System Log** > **View System Log** to view the ZyXEL Device's system logs.

Figure 70 Management > System Log > View System Log



The following table describes the fields in this screen.

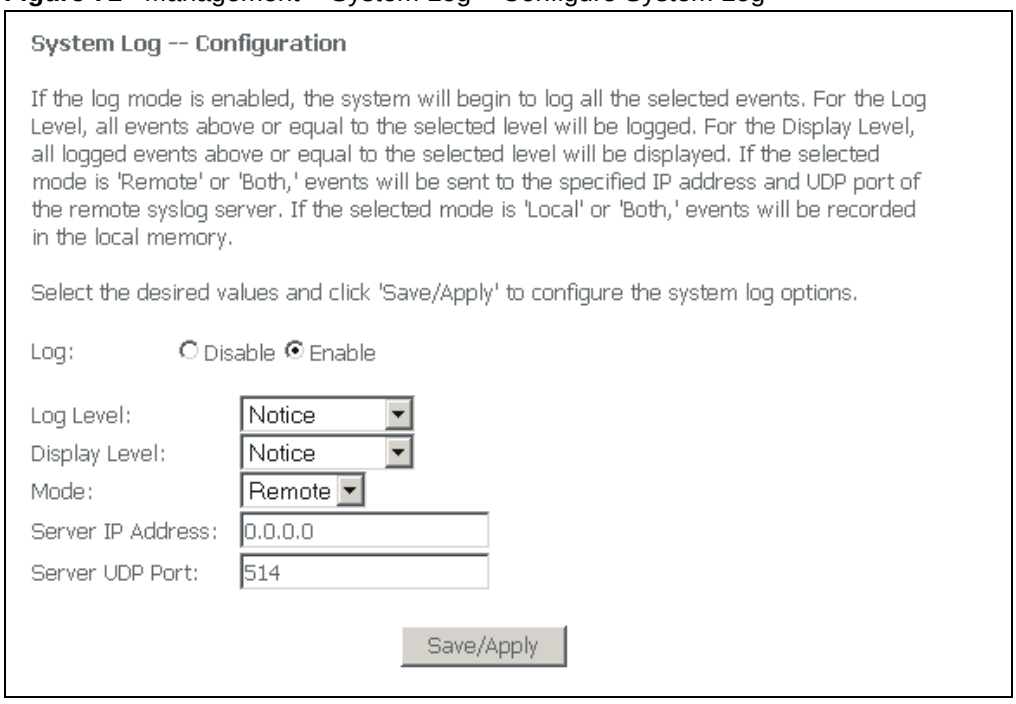
Table 50 Management > System Log > View System Log

LABEL	DESCRIPTION
Date/Time	This field displays when the log was recorded.
Facility	This is the log's category.
Severity	This is the event's degree of seriousness.
Message	This field states the reason for the log.
Refresh	Click **Refresh** to renew the log screen.
Close	Click this to close the window.

18.4 Configuring Log Settings

Click **Management** > **System Log** > **Configure System Log** to display the following screen. Use this screen to configure the level of events to log and where to send logs.

Figure 71 Management > System Log > Configure System Log


System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log:
Disable
Enable
Log Level:
Notice
Display Level:
Notice
Mode:
Remote
Server IP Address:
0.0.0.0
Server UDP Port:
514
Save/Apply

The following table describes the fields in this screen.

Table 51 Management > System Log > Configure System Log

LABEL	DESCRIPTION
Log	This controls whether or not the ZyXEL Device logs events.
Log Level	Select the lowest level of events that you want the ZyXEL Device to log. The ZyXEL Device logs all events with that severity level or higher.
Display Level	Select the lowest level of events that you want the ZyXEL Device to display. The ZyXEL Device displays events with that severity level or higher.
Mode	Select **Local** to only record events in the ZyXEL Device's memory. Select **Remote** to send events to a remote syslog server. Select **Both** to record events in the ZyXEL Device's memory and send them to a remote syslog server.
Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Server UDP Port	Enter the UDP port number the ZyXEL Device is to use when sending syslog events to the syslog server.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

19

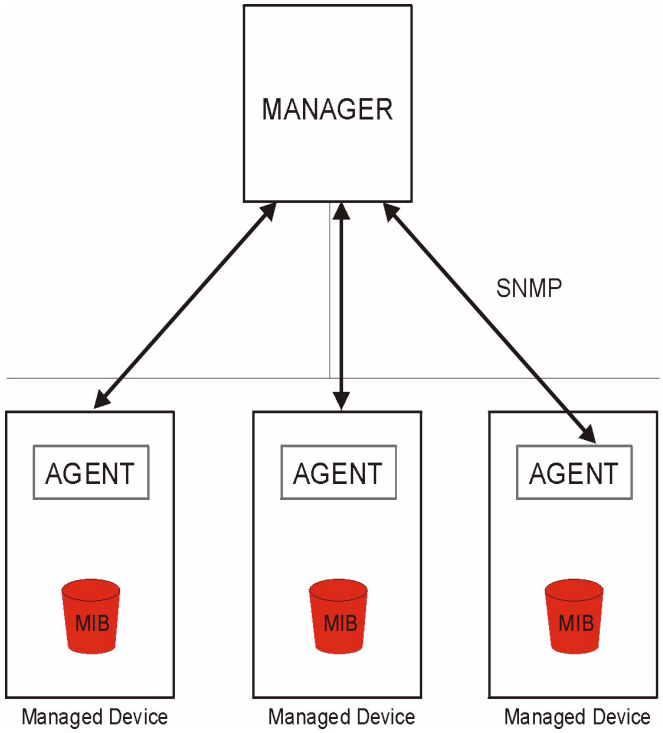
SNMP

This chapter provides information on the SNMP screen.

19.1 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of TCP/IP protocol suite. A manager station can monitor the ZyXEL Device through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 72 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 52 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Trap	Used by the agent to inform the manager of some events.

19.1.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance. The ZyXEL Device supports the following MIBs:

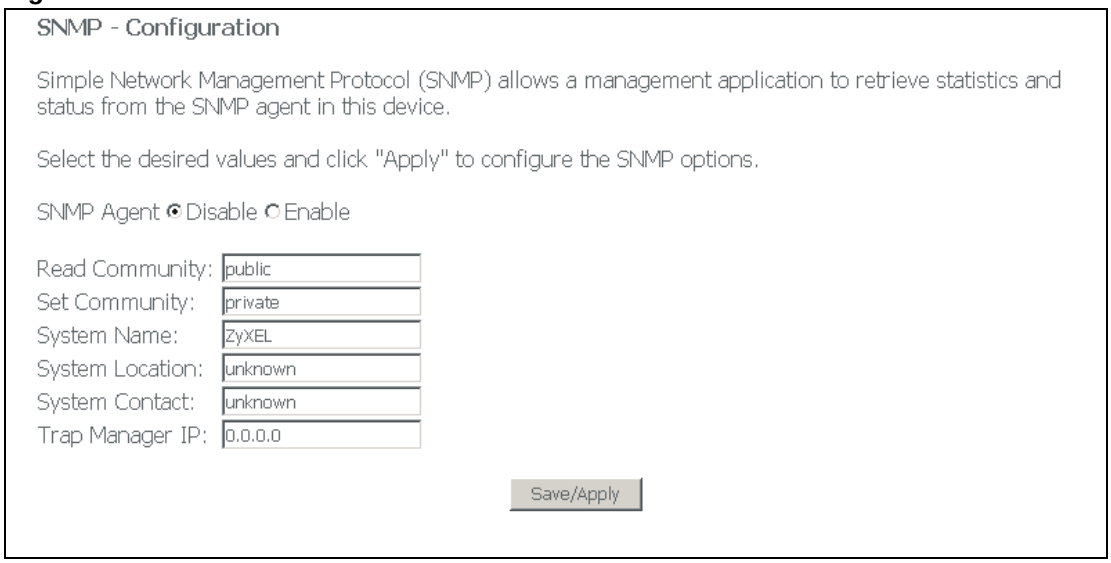
- ADSL mib
- AT mib
- ATM mib
- ICMP mib
- IP mib
- SNMP mib
- SYSOR mib
- TCP mib
- UDP mib

The ZyXEL Device uses these MIBs to provide read-only information. You cannot use SNMP to configure the ZyXEL Device.

19.2 SNMP Screen

To open this screen, click **Advanced Application**, **Access Control**, **SNMP**.

Figure 73 SNMP


SNMP - Configuration
Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.
Select the desired values and click "Apply" to configure the SNMP options.
SNMP Agent Disable Enable
Read Community: public
Set Community: private
System Name: ZyXEL
System Location: unknown
System Contact: unknown
Trap Manager IP: 0.0.0.0
Save/Apply

The following table describes the labels in this screen.

Table 53 SNMP

LABEL	DESCRIPTION
SNMP Agent	Enable the SNMP agent to turn on SNMP on the ZyXEL Device.
Read Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
System Name	Specify the name the ZyXEL Device uses for SNMP.
System Location	Specify where the ZyXEL Device is.
System Contact	Specify the name of the person administering the ZyXEL Device.
Trap Manager IP	Enter the IP address of a station to send your SNMP traps to. The ZyXEL Device sends a coldStart trap when the power is turned on.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.
Port	Enter the port number upon which the station listens for SNMP traps.

20

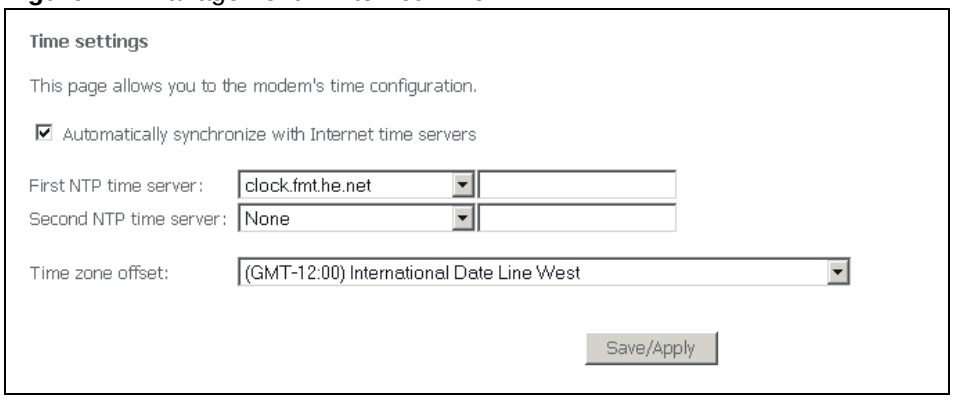
Time

This chapter covers how to set the time in the ZyXEL Device.

20.1 Time Setup

Click **Management** > **Internet Time** to open the following screen. Use this screen to configure how the ZyXEL Device synchronizes its internal clock with a time server on the Internet.

Figure 74 Management > Internet Time



The following table describes the labels in this screen.

Table 54 Management > Internet Time

LABEL	DESCRIPTION
Automatically synchronize with Internet time servers	Select this radio button to have the ZyXEL Device get the time and date from the NTP time server you specify. See RFC 1305 for details on NTP.
First NTP time server	Enter the IP address or URL of the time server that the ZyXEL Device should use to update time and date settings.
Second NTP time server	Enter the IP address or URL of the time server that the ZyXEL Device should use to update time and date settings if it cannot get a response from the first time server.
Time Zone	Choose the time zone of your location. This sets the time difference between your time zone and Greenwich Mean Time (GMT).
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

21

Access Control

This chapter describes how to configure access control.

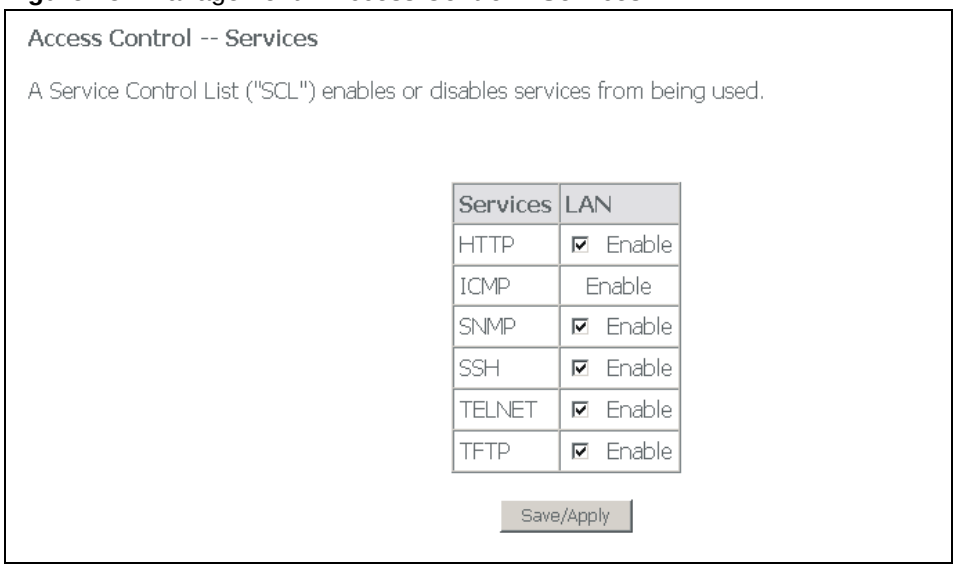
21.1 Access Control Screen

Use the access control screens to enable or disable service access to the ZyXEL Device.

21.2 Service Access Control Screen

To open this screen, click **Management > Access Control** > **Services**.

Figure 75 Management > Access Control > Services



The following table describes the labels in this screen.

Table 55 Management > Access Control > Services

LABEL	DESCRIPTION
Services	Services you may use to access the ZyXEL Device are listed here.

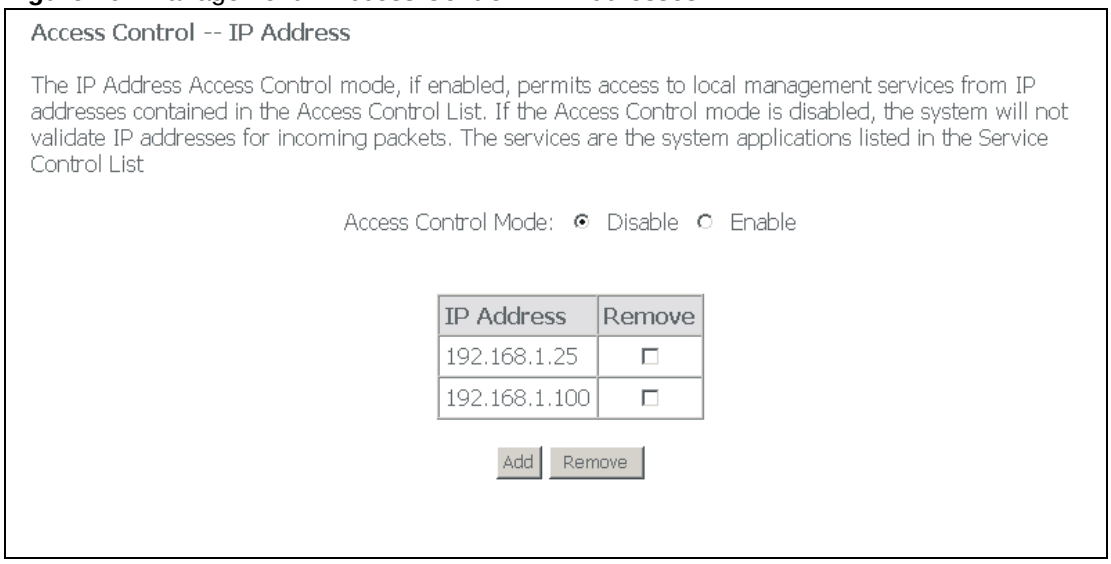
Table 55 Management > Access Control > Services

LABEL	DESCRIPTION
LAN	Select the **Enable** check boxes for the corresponding services that you want to allow to access the ZyXEL Device from the LAN.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

21.3 IP Addresses

This screen lists the IP addresses of trusted computers that may manage the ZyXEL Device. To open this screen, click **Management** > **Access Control** > **IP Addresses**.

Figure 76 Management > Access Control > IP Addresses


Access Control -- IP Address
The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List
Access Control Mode: Disable Enable
IP Address
Remove
192.168.1.25
192.168.1.100
Add
Remove

The following table describes the labels in this screen.

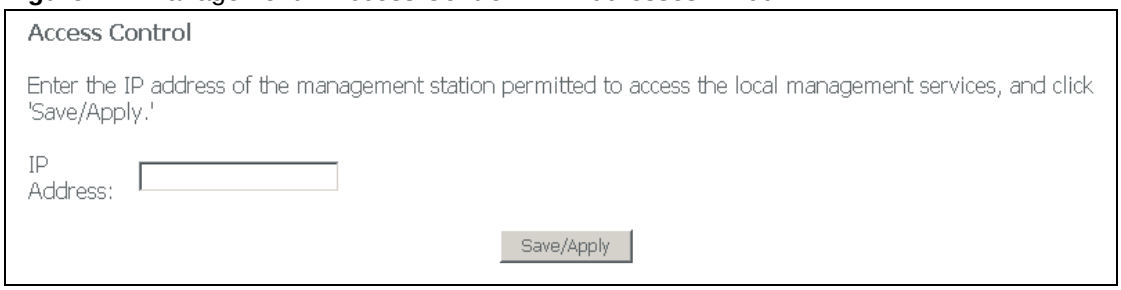
Table 56 Management > Access Control > IP Addresses

LABEL	DESCRIPTION
Access Control Mode	Enable this to have the ZyXEL Device check the source IP address of incoming local management sessions.
IP Address	This is the IP address of a trusted computer from which you can manage the ZyXEL Device.
Remove	To remove an entry, select its **Remove** check box and click the **Remove** button.
Add	Click this button to go to a screen where you can configure settings for a new trusted IP address.

21.4 Adding IP Addresses

Use this screen to add IP addresses of trusted computers that may manage the ZyXEL Device. To open this screen, click **Management > Access Control** > **IP Addresses > Add**.

Figure 77 Management > Access Control > IP Addresses > Add


Access Control
Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'
IP Address:
Save/Apply

The following table describes the labels in this screen.

Table 57 Management > Access Control > IP Addresses > Add

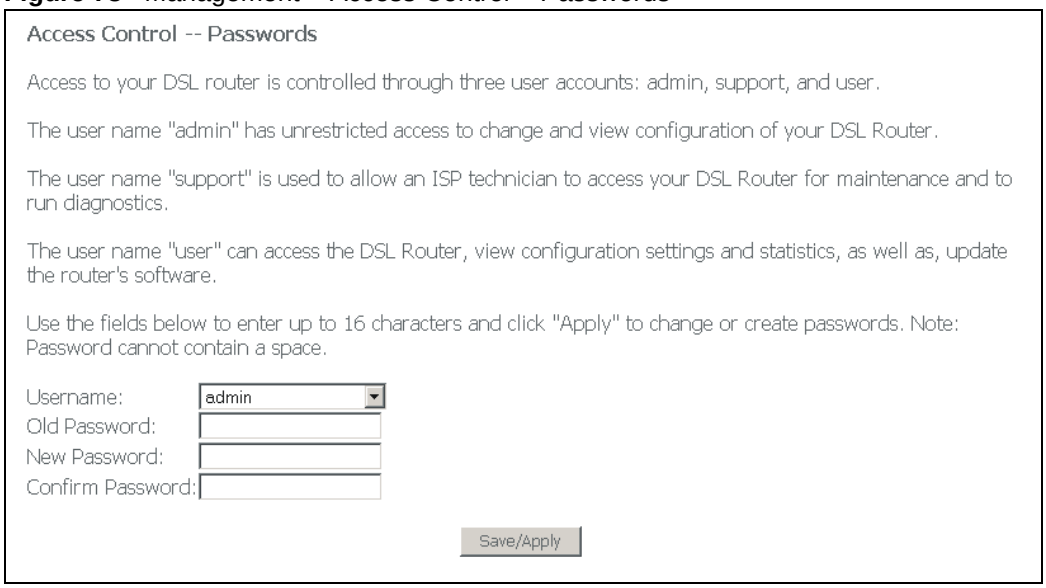
LABEL	DESCRIPTION
IP Address	Specify the IP address of a trusted computer from which you want to manage the ZyXEL Device.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

21.5 Passwords

Click **Management > Access Control** > **Passwords** to open the following screen. Use this screen to configure the ZyXEL Device's passwords.

The "support" user name and password for ISP technician login only works through the DSL connection.

Figure 78 Management > Access Control > Passwords


Access Control -- Passwords
Access to your DSL router is controlled through three user accounts: admin, support, and user.
The user name "admin" has unrestricted access to change and view configuration of your DSL Router.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
Username:
admin
Old Password:
New Password:
Confirm Password:
Save/Apply

The following table describes the labels in this screen.

Table 58 Management > Access Control > Passwords

LABEL	DESCRIPTION
Username	Select the user name for which you want to configure the password. The **admin** or **user** account can only access the ZyXEL Device from the LAN. The **support** account can only access the ZyXEL Device from the WAN. Only the **admin** or **support** account can use Telnet to log into the ZyXEL Device.
Old Password	Type the existing password.
New Password	Type the new password. Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Confirm Password	Type the new password again to make sure it is entered properly.
Save/Apply	Click this button to save the changes and have the ZyXEL Device start using them.

22

Update Software

This chapter covers upgrading the ZyXEL Device's firmware.

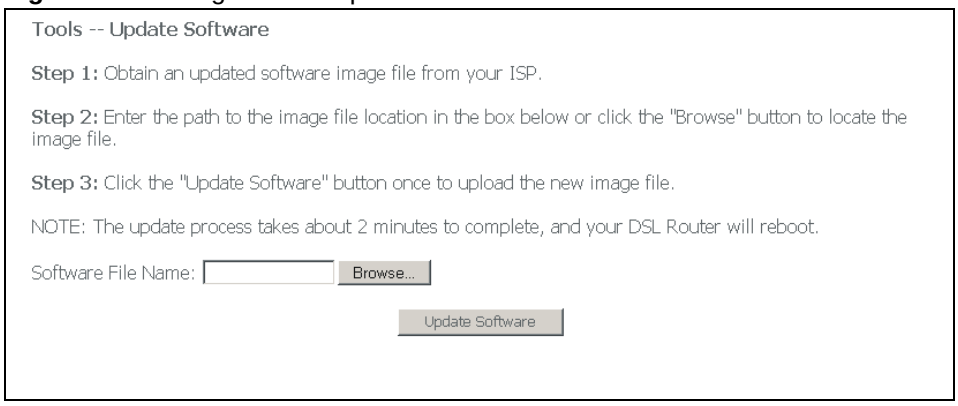
22.1 Uploading Firmware

The software embedded in the ZyXEL Device is called "firmware". Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "ZyXEL Device.bin". The upload process described here may take up to two minutes. After a successful upload, the system will reboot.

Only use firmware for your device's specific model. Refer to the label on the bottom of your device.

Click **Management** > **Update Software** to open the following screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 79 Management > Update Software


Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
Software File Name:
Browse...
Update Software

The following table describes the labels in this screen.

Table 59 Management > Update Software

LABEL	DESCRIPTION
Software File name	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.

Table 59 Management > Update Software (continued)

LABEL	DESCRIPTION
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Update Software	Click **Upload** to begin the upload process. This process may take up to two minutes.

Do NOT turn off the ZyXEL Device while firmware upload is in progress!

After you upload firmware, wait before logging into the ZyXEL Device again. The ZyXEL Device automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 80 Network Temporarily Disconnected

After the ZyXEL Device finishes restarting, log in again and check your new firmware version in the **Status** screen.

23

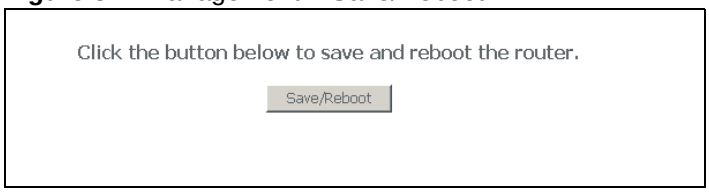
Save/Reboot and Logout

This chapter covers the save and reboot screen.

23.1 Save/Reboot

Click **Management** > **Save/Reboot** to open the following screen. Click **Save/Reboot** to save all of your ZyXEL Device's settings and reboot the ZyXEL Device without turning the power off.

Figure 81 Management > Save/Reboot



23.2 Logout

Click **Management** > **Logout** to exit the web configurator.

PART IV
Troubleshooting and Specifications

Troubleshooting (143)
Product Specifications (147)

24

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access

24.1 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure the ZyXEL Device is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
3. Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 28.
2. Check the hardware connections. See Section 1.4 on page 27.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

24.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1. The default IP address is 192.168.1.1.
2. If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 33.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 33.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address (Section 6.2.1 on page 68), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.4 on page 27 and Section 1.5 on page 28.
3. Make sure your Internet browser does not block pop-up windows. See Appendix C on page 181.
4. Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)
   - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 6.2.1 on page 68. Your ZyXEL Device is a DHCP server by default.
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device. See Section 6.2.1 on page 68.
5. Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 2.3 on page 33.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the user name and password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
2 Turn the ZyXEL Device off and on.
3 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 33.

24.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.4 on page 27 and Section 1.5 on page 28.
2 If your ISP gave you Internet connection information, make sure you entered it correctly in the **Network** > **WAN** > **Internet Connection** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3 Disconnect all the cables from your device, and follow the directions in Section 1.4 on page 27 again.
4 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.4 on page 27 and Section 1.5 on page 28.
2 Reboot the ZyXEL Device.
3 Turn the ZyXEL Device off and on.
4 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 28. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Reboot the ZyXEL Device.
3. Turn the ZyXEL Device off and on.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

25

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Table 60 Device Specifications

Dimensions (W x D x H)	50.4 x 207 x 160.8 mm
Power Specification	12 VDC 1.5 A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X (auto-crossover) 10/100 Mbps RJ-45 Ethernet ports
Operating Temperature	0º C ~ 40º C
Storage Temperature	-30º ~ 60º C
Operating Humidity	20%~85% (non-condensing)
Storage Humidity	10%~95% (non-condensing)

Table 61 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Admin User Name	admin
User User Name	user
Support User Name	support
Default Password	1234
ADSL Standards	Multi-Mode standard (ANSI T1.413,Issue 2; G.dmt(G.992.1); G.lite(G992.2)). ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) MAC encapsulated routing (ENET encapsulation) VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) OAM F4/F5 end-to-end loopback, AIS, and RDI OAM cells ATM-based Multi-Pair Bonding (G.998.1) support

Table 61 Firmware Specifications

FEATURE	DESCRIPTION
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol. Transparent bridging for unsupported network layer protocols. DHCP Server/Client/Relay RIP I / RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy UPnP
Management	Use the embedded web configurator to easily configure the rich range of features on the ZyXEL Device. SNMP manageable Syslog Built-in diagnostic tools for ADSL circuitry and LAN ports
Firewall	Block traffic originating from the Internet from accessing the LAN. Protects against DoS and DDoS attacks, including SYNC flooding, IP Smurf, Ping of Death, Fraggle, Teardrop, and Land attacks.
NAT	Virtual Server (Port Forwarding) Port Triggering DMZ Host IP
Other Features	Dynamic DNS Static Routes
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Virtual Server	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. These dates and times are then used in logs.
Syslog	The ZyXEL Device can send syslogs to an external syslog server.
PPPoE	PPPoE mimics a dial-up Internet access connection.

Table 61 Firmware Specifications

FEATURE	DESCRIPTION
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	You can configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Access Control	This allows you to decide whether a service (HTTP traffic for example) from a computer on the LAN can access the ZyXEL Device.

Table 62 Standards Supported

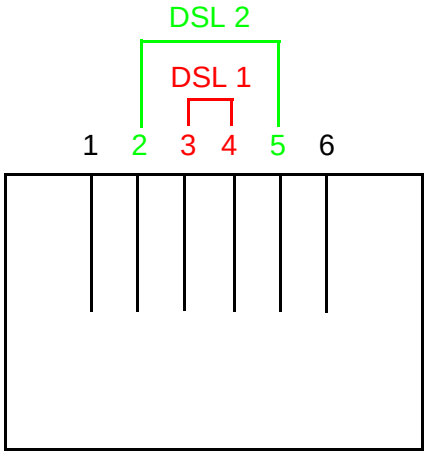
STANDARD	DESCRIPTION
RFC 1483/2684 (MPOA)	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2364 (PPPoA)	PPP over AAL5
RFC 2516 (PPPoE)	PPP over Ethernet
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard
ITU G.992.1 (G.dmt)	ITU standard for ADSL using discrete multitone modulation
ITU G.992.2 (G. lite)	ITU standard for ADSL using discrete multitone modulation
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.3 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
ITU G.998.1 (G.bond ATM)	ATM-based Multi-Pair Bonding
RFC 1112 (IGMP v1)	Internet Group Management Protocol, Version 1
RFC 2236 (IGMP v2)	Internet Group Management Protocol, Version 2
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 1305	Network Time Protocol (Version 3) Specification, Implementation
RFC 1334 (PAP)	PPP Authentication Protocols
RFC 1994 (CHAP)	PPP Challenge Handshake Authentication Protocol
RFC 1332 (IPCP)	The PPP Internet Protocol Control Protocol
RFC 1058 (RIP-1)	Routing Information Protocol
RFC 1723 (RIP-2)	RIP Version 2 - Carrying Additional Information
RFC 1631 (NAT)	IP Network Address Translator
RFC 1661 (PPP)	The Point-to-Point Protocol
RFC 1157 (SNMPv1)	Simple Network Management Protocol, Version 1
RFC 1441 (SNMPv2)	Simple Network Management Protocol, Version 2
RFC 2408 (ISAKMP)	Internet Security Association and Key Management Protocol

25.1 DSL Connector Pin Assignments

The ZyXEL Device's RJ-11 DSL connector handles both the DSL 1 and DSL 2 connections.

- Pins 3 and 4 are for DSL 1.
- Pins 2 and 5 are for DSL 2.

Figure 82 DSL Connector Pin Assignments



25.2 Power Adaptor Specifications

Table 63 North American Plug Standards

AC POWER ADAPTOR MODEL	PSA18R-120P (ZA)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	UL, CUL (UL 60950-1 FIRST EDITIONCSA C22.2 NO. 60950-1-03 1ST.)

Table 64 European Plug Standards

AC POWER ADAPTOR MODEL	PSA18R-120P (ZE)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	TUV, CE (EN 60950-1)

Table 65 United Kingdom Plug Standards

AC POWER ADAPTOR MODEL	PSA18R-120P (ZK)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A

Table 65 United Kingdom Plug Standards

POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	TUV (BS EN 60950-1)

PART V
Appendices and Index

Setting up Your Computer's IP Address (155)
IP Addresses and Subnetting (171)
Pop-up Windows (181)
Common Services (185)
Legal Information (189)
Customer Support (193)
Index (199)

A

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

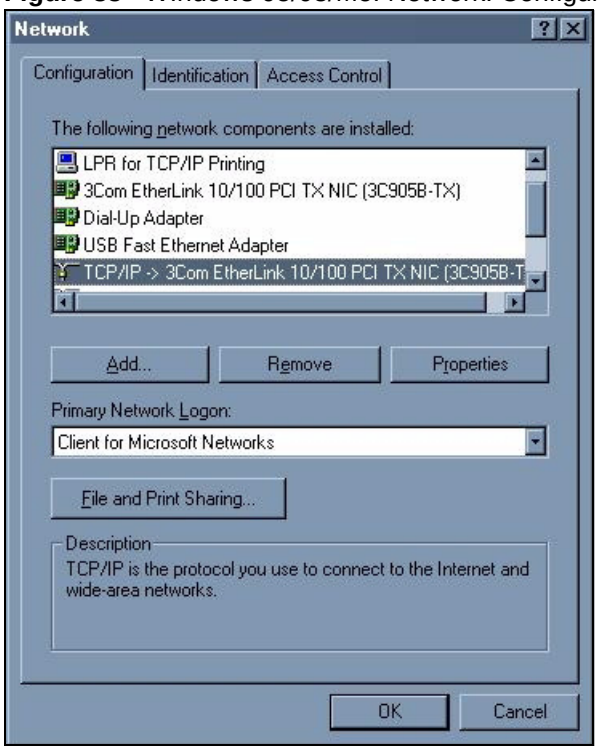
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 83 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

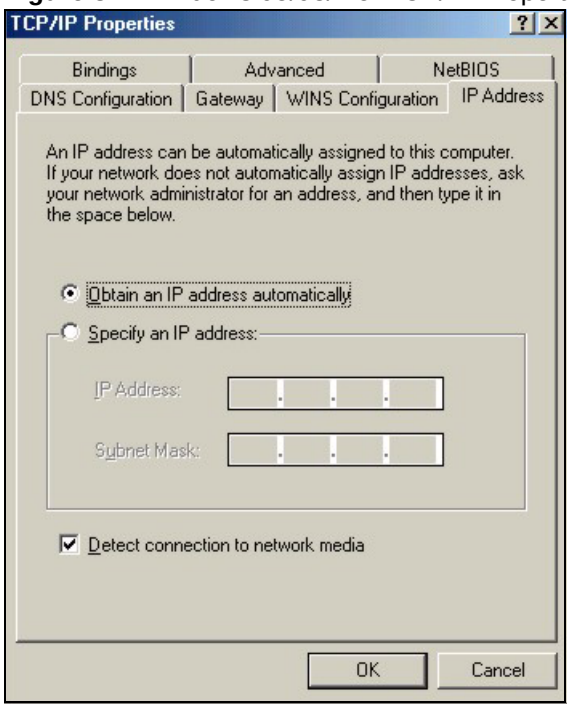
If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

Configuring

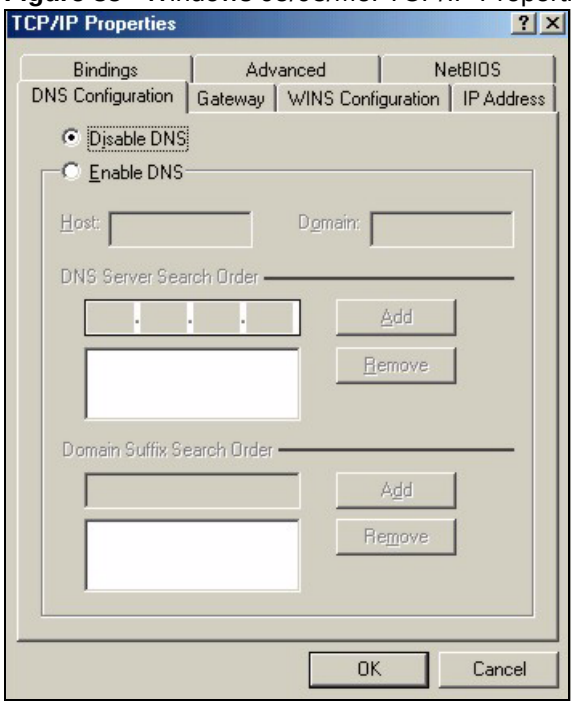
1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
2. Click the **IP Address** tab.
   - If your IP address is dynamic, select **Obtain an IP address automatically**.
   - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 84 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3. Click the **DNS** Configuration tab.
   - If you do not know your DNS information, select **Disable DNS**.
   - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 85 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your ZyXEL Device and restart your computer when prompted.

Verifying Settings

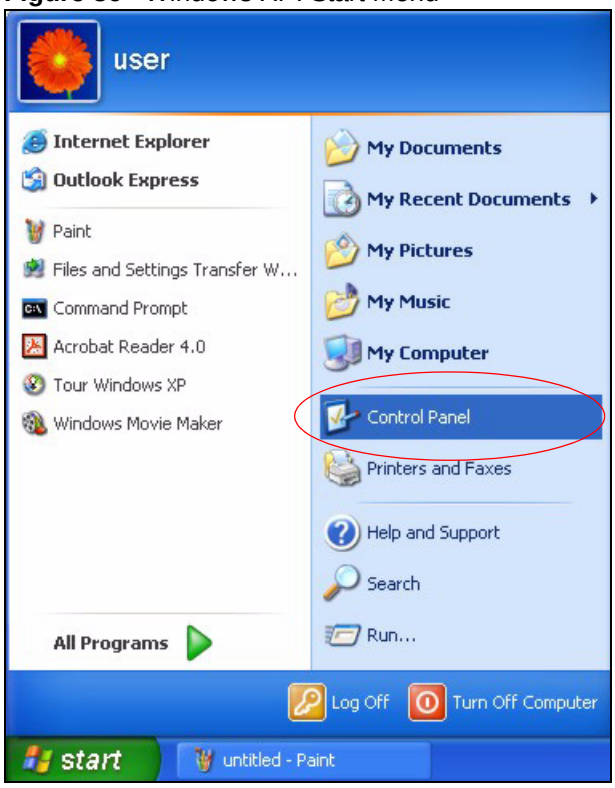
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 86 Windows XP: Start Menu

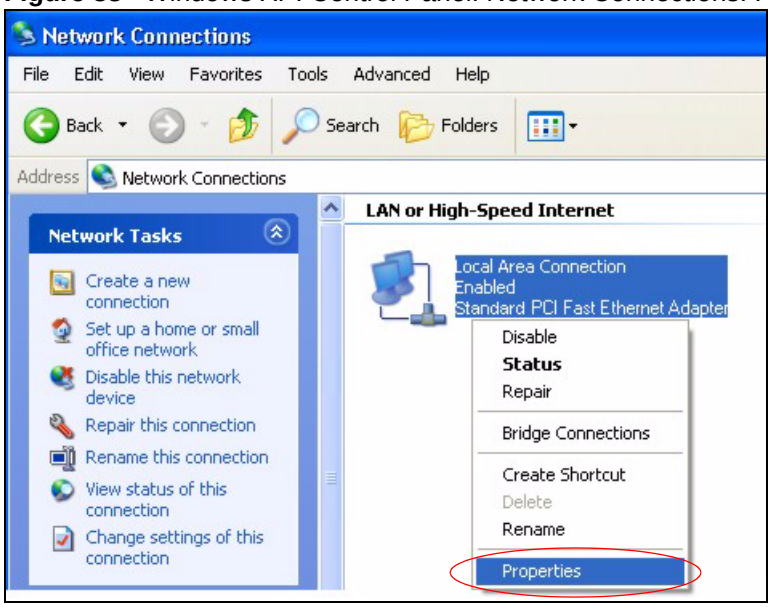


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 87 Windows XP: Control Panel

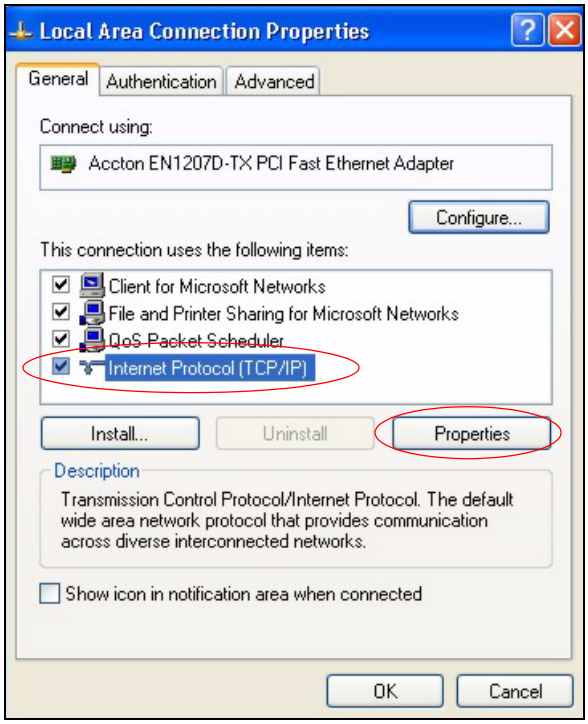
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 88 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

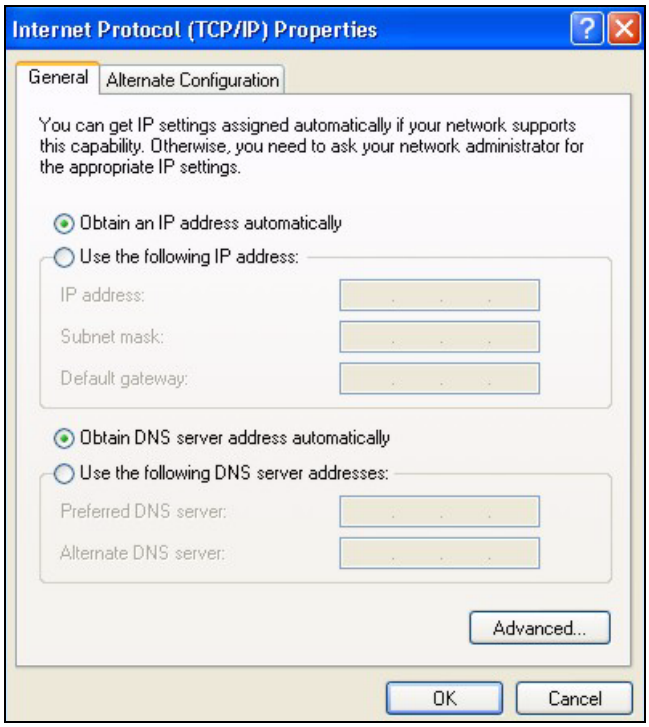
Figure 89 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 90 Windows XP: Internet Protocol (TCP/IP) Properties

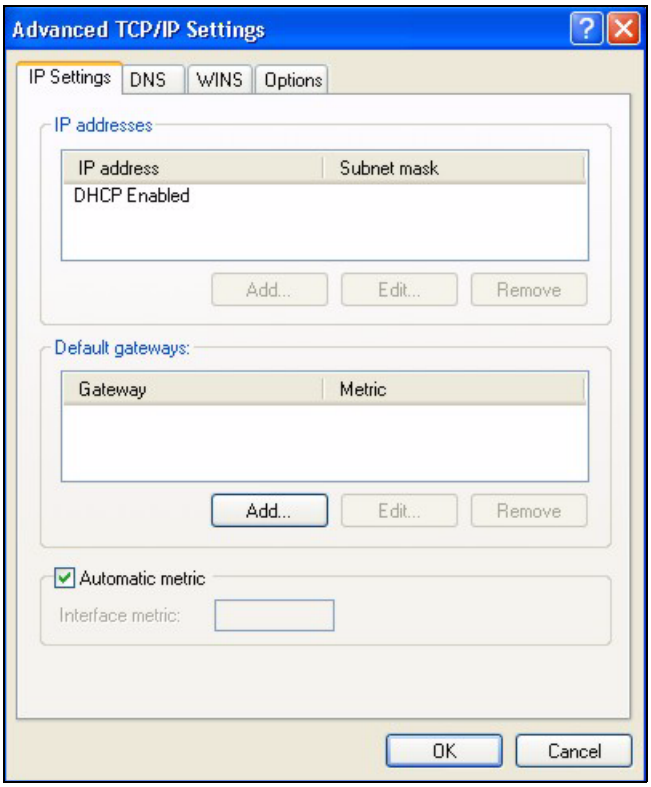

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 91 Windows XP: Advanced TCP/IP Properties

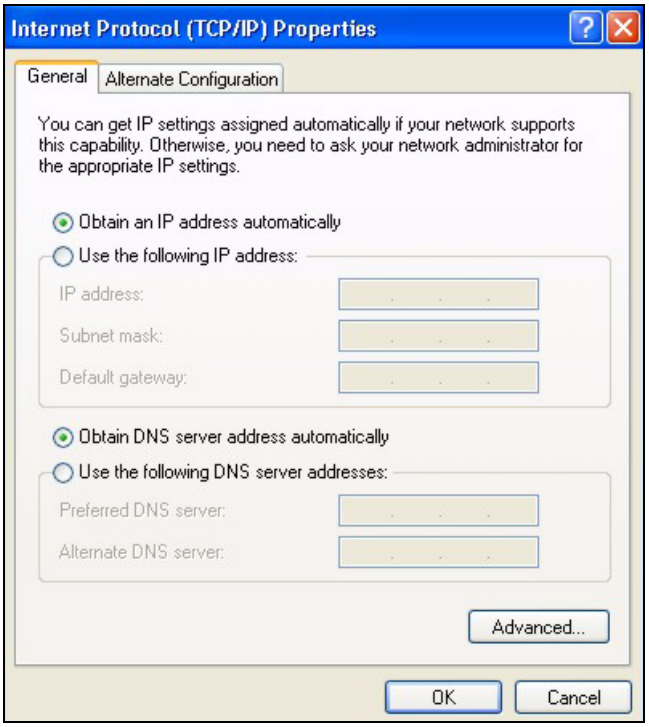


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 92 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

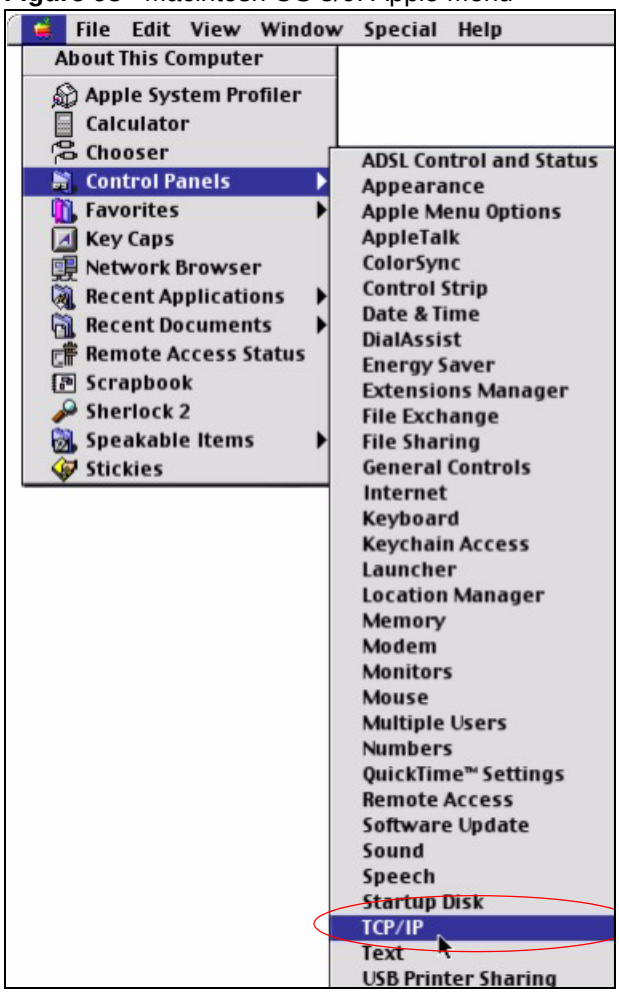
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

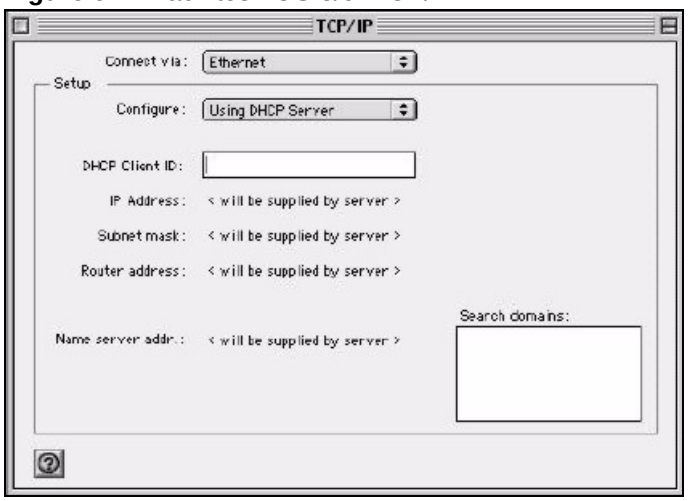
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 93 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 94 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL Device and restart your computer (if prompted).

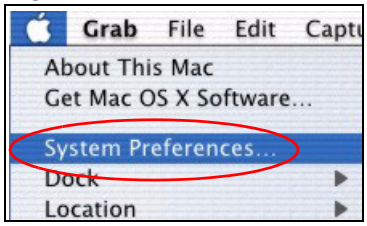
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 95 Macintosh OS X: Apple Menu

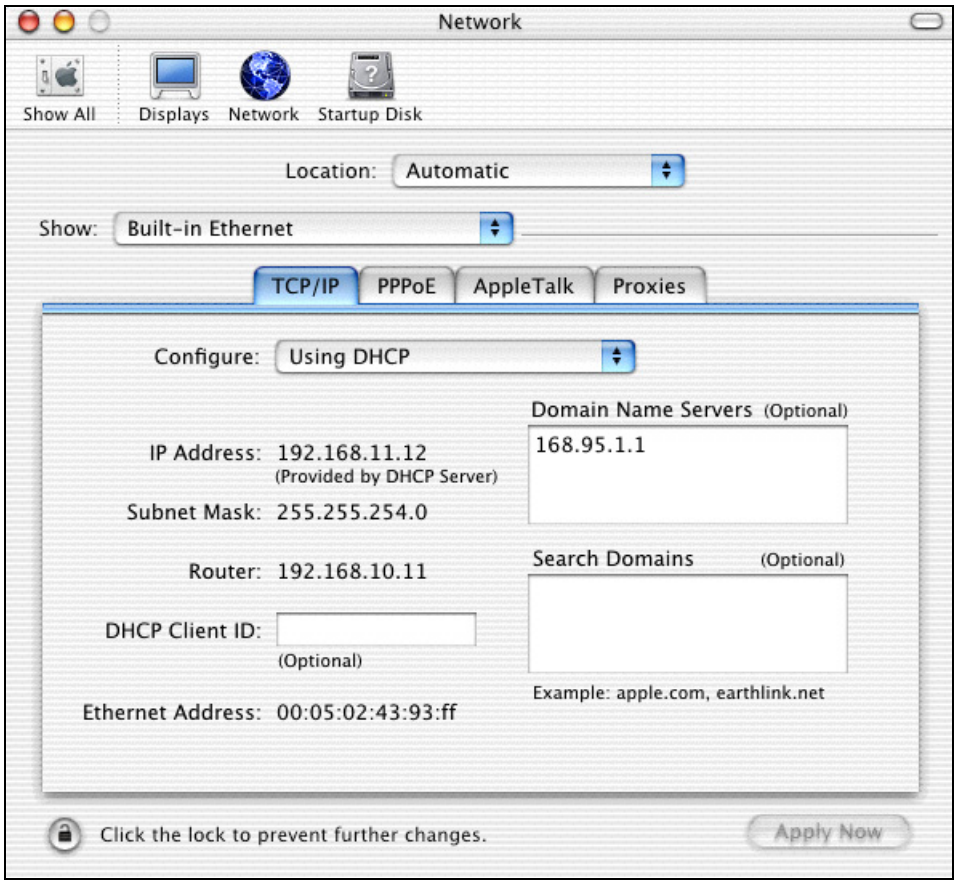


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 96 Macintosh OS X: Network



4 For statically assigned settings, do the following:
   - From the **Configure** box, select **Manually**.
   - Type your IP address in the **IP Address** box.
   - Type your subnet mask in the **Subnet mask** box.
   - Type the IP address of your ZyXEL Device in the **Router address** box.
5 Click **Apply Now** and close the window.
6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

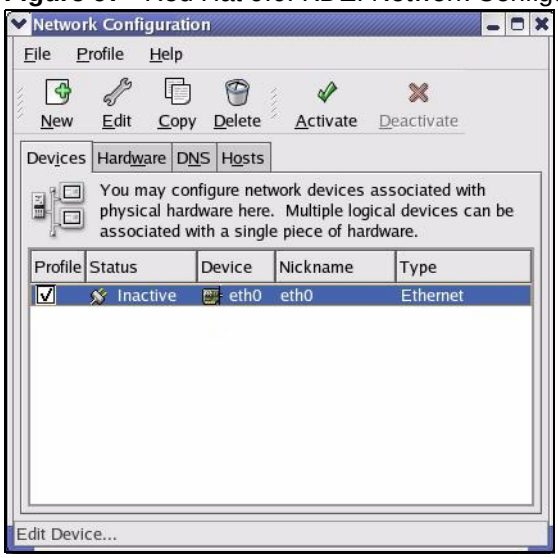
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 97 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

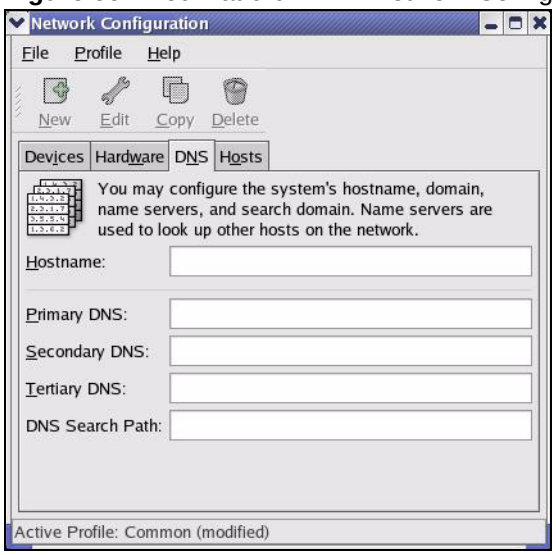
Figure 98 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

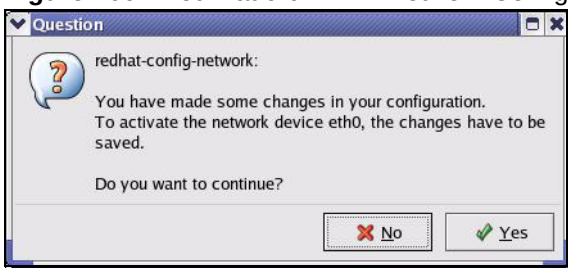
Figure 99 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 100 Red Hat 9.0: KDE: Network Configuration: Activate


Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 101 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 102 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2. If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 103 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3. After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 104 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 105 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

B

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

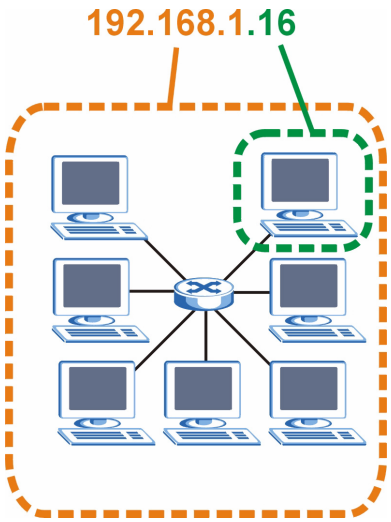
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 106 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 66 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 67 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 68 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 69 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 69 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

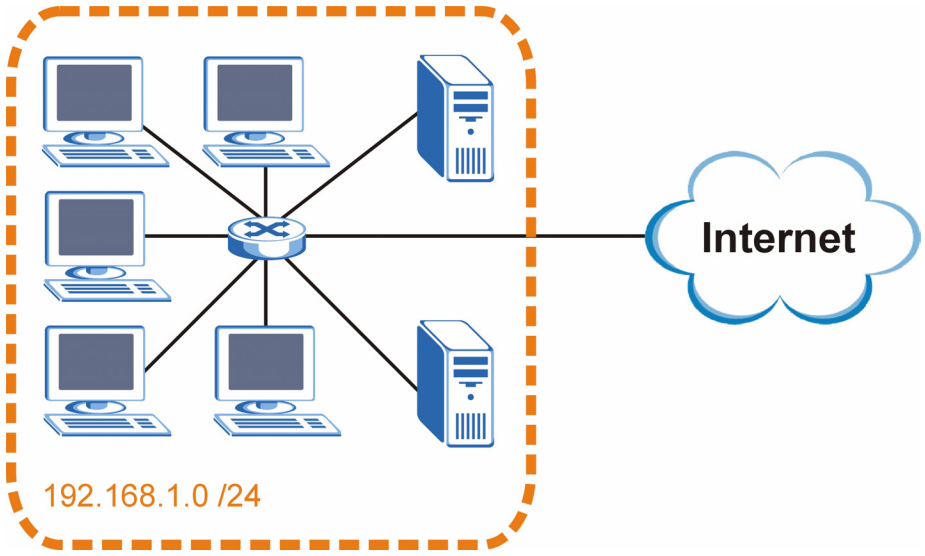
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 107 Subnetting Example: Before Subnetting

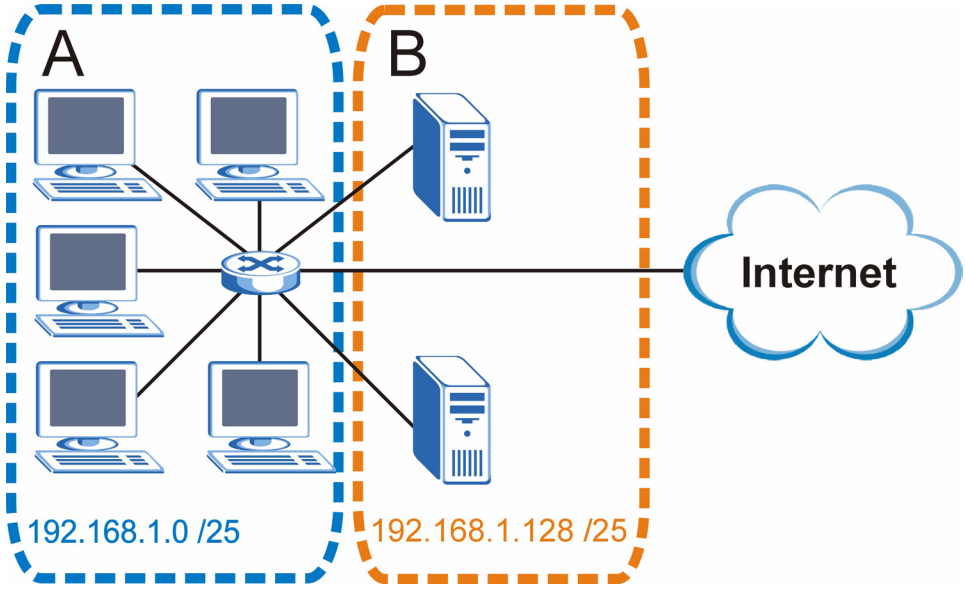


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 108 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 70 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 71 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 72 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 73 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 74 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 74 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 75 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 76 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 76 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

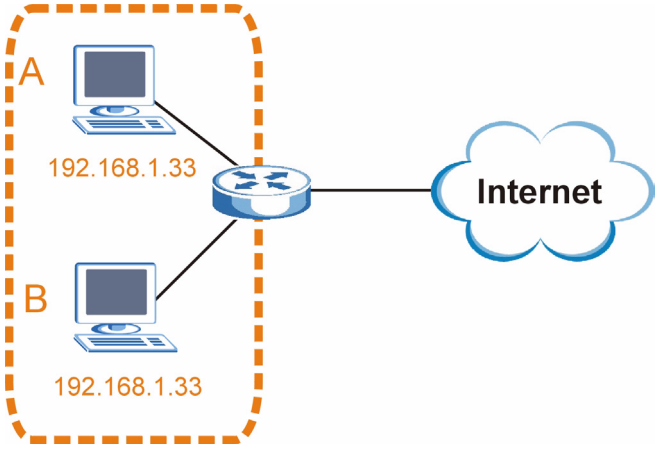
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

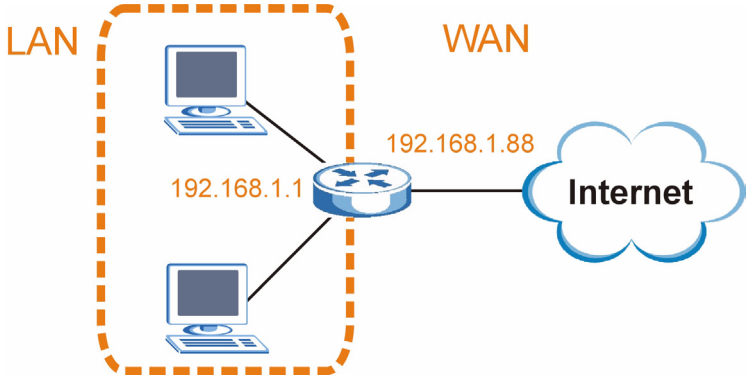
Figure 109 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

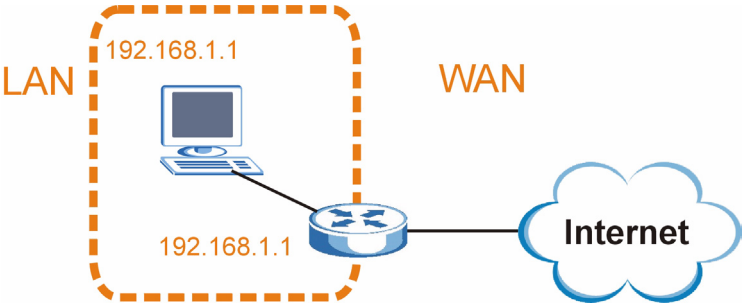
Figure 110 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 111 Conflicting Computer and Router IP Addresses Example



C

Pop-up Windows

In order to use the web configurator you need to allow web browser pop-up windows from your device.

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

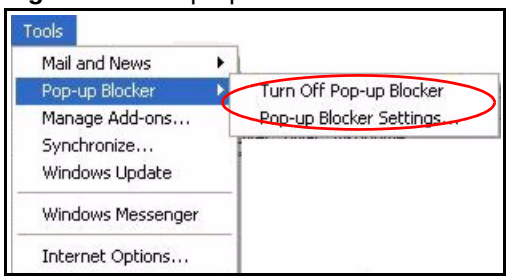
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1. In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

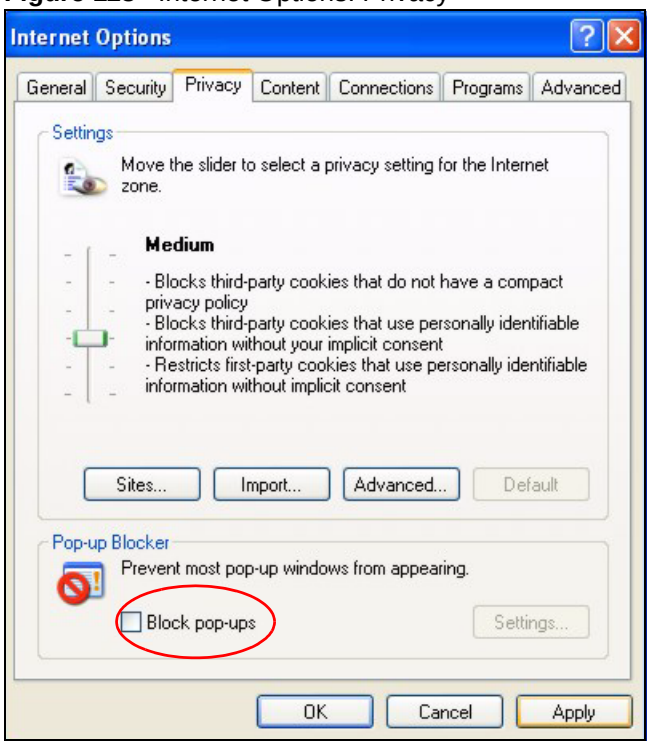
Figure 112 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1. In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.
2. Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 113 Internet Options: Privacy



3 Click **Apply** to save this setting.

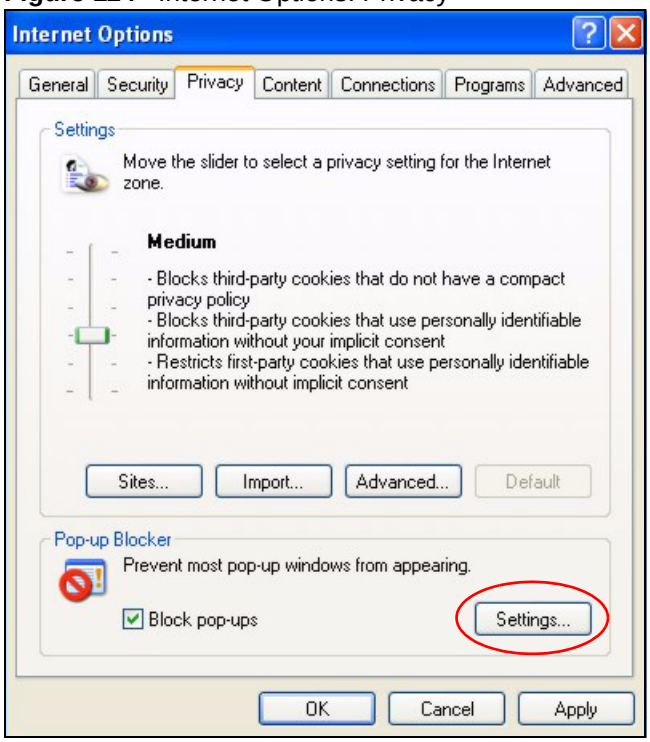
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 114 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 115 Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

D

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 77 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 77 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.

Table 77 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

E

Legal Information

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of

ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

F

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

Numerics

10/100 Mbps **147**

A

access control **133**
  adding IP addresses **135**
  IP addresses **134**
  passwords **135**
  services **133**
ADSL setup **109**
ADSL standards **147**
ADSL synchronization test **117**
alternative subnet mask notation **173**
ATM Adaptation Layer 5 (AAL5) **56**
auto MDI/MDI-X **147**
auto-crossover **147**
auto-negotiating **147**

B

backing up configuration **119**
backup settings **119**
blocking schedule **86**
bridging groups **111**
broadcast **63**

C

certifications **189**
  notices **190**
  viewing **190**
Class of Service (CoS) **90**
configuration **68**, **168**
  backup **119**
  restore **119**
configuration backup **119**
connection type **57**
contact information **193**
copyright **189**
CoS **90**
CoS (class of service) **90**
customer support **193**

D

default **120**
default gateway **97**
default LAN IP address **31**
device management **26**
device model number **137**
DHCP **47**, **68**, **148**
DHCP vendor IDs **113**
diagnostics **117**
DiffServ (Differentiated Services) **90**
DiffServ Code Point (DSCP) **90**
DiffServ marking rule **91**
dimensions **147**
disclaimer **189**
DMZ host **80**
DNS **103**
domain name system
  see DNS
double upstream mode **109**
DS field **90**
DS See Differentiated Services
DSCP **90**
DSL connector pin assignments **150**
DSL setup **109**
dynamic DNS **105**
Dynamic Host Configuration Protocol. See DHCP.
DYNDNS wildcard **105**

E

Encapsulation **55**
  ENET ENCAP **56**
  PPP over Ethernet **56**
  PPPoA **56**

RFC 1483 56
Ethernet adapter card 155
Ethernet connection test 117
Ethernet ports 147

F

FCC interference statement 189
filename
extension 137
filtering 81, 82, 84
firewall 148
firmware 25, 137
upgrade 137
upload 137

G

GMT 131
Greenwich Mean Time. See GMT.

H

hub 25, 147
humidity 147

I

IANA 68, 69, 178
IGMP 64, 69
version 64
incoming IP filtering 82
Internet access 25
Internet access blocking 86
Internet Assigned Numbers Authority
See IANA 178
see IANA 68
Internet Group Management Protocol
see IGMP
Internet time 131
IP address 68, 147
IP addresses
access control 134
adding in access control 135
IP filtering 81, 82
IP precedence 90

L

LAN
connection test 117
LAN setup 67
LAN TCP/IP 68
logs 123
configuring 124
viewing 123

M

MAC address
filter 86
filtering 84
MAC Encapsulated Routing (MER) 56
management 148
Management Information Base (MIB) 128
mapping ports to PVCs 111
Maximum Burst Size
see MBS
MBS 52
MIBs 128
multicast 63, 69
multi-mode 147
multiplexing 51, 56
LLC-based 51, 57
VC-based 51, 57
Multiprotocol Encapsulation 56

N

nailed-up connection 58
NAT 68, 73, 74, 80, 148, 178
DMZ host 80
port triggering 77
virtual servers 73
NAT traversal 70
navigating the web configurator 33
Network Address Translation
see NAT
network disconnect icon 120, 138

O

outgoing IP filtering **81**

P

parental control **86**
password **147**
passwords **135**
PCR **52**
Peak Cell Rate
see PCR
PHB (Per-Hop Behavior) **91**
pin assignments **150**
Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) **56**
Point-to Point Protocol
see PPP
port forwarding **73**
port mapping **111**
ports
Ethernet **147**
POTS **25**
power specifications **147**
PPP **148**
PPP session over Ethernet (PPP over Ethernet, RFC 2516) **56**
product registration **191**
PVC (Permanent Virtual Circuit) **56**

Q

QoS **90**
classifier **92**
classifiers **93**
queues **92**
QoS class configuration **93**
Quality of Service (QoS) **89**

R

reach extended ADSL2 **109**
registration
product **191**
related documentation **3**
reset button **33**
resetting the ZyXEL device **33**
restore configuration **119**
restore settings **119**
RFC 1058. See RIP.
RFC 1389. See RIP.
RFC 1483 **56**
RFC 1631 **73**
RFC 2131. See DHCP.
RFC 2132. See DHCP
RIP **101**
direction **101**
version **101**
RJ-45 ports **147**
Routing Information Protocol. See RIP.

S

safety warnings **6**
save settings **119**
SCR **52**
screen summary **34**
services **73**
access control **133**
settings
backup **119**
restore **119**
Simple Network Management Protocol. See SNMP.
SNMP **127**
commands **128**
Get **128**
GetNext **128**
manager **128**
MIBs **128**
supported versions **127**
Trap **128**
splitters **27**
static route **97**, **98**
subnet **171**
subnet mask **68**, **172**
subnetting **174**
switch **147**
syntax conventions **4**

T

TCP/IP **155**
temperature **147**

time
zone 131
ToS (Type of Service) 90
trademarks 189
traffic shaping 51
trigger port forwarding 77

U

unicast 63
upgrading firmware 137
uploading firmware 137
UPnP 69
application 70
security issues 70
user names 147

V

VC 51
permanent virtual circuit
see PVC
VCC 43
VCI 51
viewing system logs 123
Virtual Channel Connection (VCC) 43
Virtual Channel Identifier
see VCI
virtual circuit
see VC
virtual circuit (VC) 56
Virtual Path Identifier
see VPI
virtual ports 111
virtual servers 73
VPI 51

W

WAN 51
WAN setup 51
warranty 190
note 190
web configurator 31, 33
screen summary 34
Wide Area Network
see WAN